Додаток до
наказу Директора
ТОВ «SecBoard»
від XX.XX.2026 № XX

План заходів
щодо приведення діяльності ТОВ «SecBoard» у відповідність до вимог постанови Правління Національного банку України від 09.12.2025 № 143 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг» (далі - Положення)

№	Завдання для ТОВ «SecBoard» (далі - Товариство) щодо виконання вимог Положення	Термін виконання	Відповідальний підрозділ / працівник (виконавець) Товариства
1	Вжиття заходів із забезпечення інформаційної безпеки та кіберзахисту до об'єктів захисту, якими є: 1) інформація, що становить таємницю фінансової послуги, яка обробляється в інформаційно-комунікаційних системах Товариства; 3) інформаційно-комунікаційні системи Товариства, що підтримують основні бізнес-процеси Товариства та/або взаємодіють з інформаційними системами Національного банку України.	до 13.12.2026[1] (постійно)	
2	Вжиття заходів із забезпечення інформаційної безпеки та кіберзахисту на всіх стадіях життєвого циклу інформаційно-комунікаційних систем Товариства.	до 13.12.2026 (постійно)	
3	Запровадження та здійснення процесу управління кіберризиками та ризиками інформаційної безпеки (Товариство має право запровадити процес в межах своєї системи управління ризиками).	до 13.12.2026 (постійно)	
4	Запровадження, використовуючи ризик-орієнтований підхід, заходи із забезпечення інформаційної безпеки та кіберзахисту, визначені в Положенні, з урахуванням	до 13.12.2026 (постійно)	

[1] **до 13.12.2026** – згідно вимог пункту 2 постанови Правління Національного банку України від 09.12.2025 № 143 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг» (тобто протягом **12 місяців із дня набрання чинності цією постановою** привести свою діяльність у відповідність до вимог Положення (згідно пункту 5 вищезазначена **постанова набрала чинності з дня, наступного за днем її офіційного опублікування; опубліковано 12.12.2025**))

	особливостей функціонування інформаційно-комунікаційних систем Товариства.		
5	Розроблення/актуалізація шаблону договору з особами, залученими для виконання заходів із забезпечення інформаційної безпеки та з реагування на інциденти інформаційної безпеки та інциденти кібербезпеки, в якому обов'язково передбачити: - норми про нерозголошення інформації (NDA, англійською мовою «Non-disclosure agreement»).	до 13.12.2026 (постійно)	
6	Здійснення перевірки особи(іб), залученої(их) для виконання заходів із забезпечення інформаційної безпеки та з реагування на інциденти інформаційної безпеки та інциденти кібербезпеки, яка(і) не може(уть) бути юридичною особою, фізичною особою-підприємцем, що є резидентами держави-агресора чи держави, що здійснює / здійснювала збройну агресію проти України, або мають кінцевих бенефіціарних власників, які є резидентами держави-агресора або держави, що здійснює / здійснювала збройну агресію проти України, або здійснюють обробку або зберігання даних за допомогою технології хмарних обчислень та центрів обробки даних, що розміщені на території держави-агресора, держави, що здійснює / здійснювала збройну агресію проти України, тимчасово окупованій території України, та/або належать суб'єктам, діяльність яких підпадає під дію Закону України «Про санкції» (далі – Закон про санкції) та стосовно яких прийнято рішення про застосування санкцій в Україні.	до 13.12.2026 (постійно)	
7	Забезпечення використання програмних, апаратних, програмно-апаратних засобів у складі інформаційно-комунікаційних систем Товариства з урахуванням вимог Закону про санкції, Закону про захист інформації, Закону про забезпечення кібербезпеки, інших законів України.	до 13.12.2026 (постійно)	

8	Керівник Товариства: 1) здійснює загальну організацію діяльності з виконання вимог з інформаційної безпеки та кіберзахисту; 2) призначає відповідальну особу за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту Товариства (окремим рішенням), здійснює контроль за його діяльністю або особисто виконує функції відповідальної особи за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту Товариства; 3) затверджує внутрішні документи з питань забезпечення інформаційної безпеки та кіберзахисту, включаючи політику, положення, стандарти, інструкції, методики, правила, стратегії, розпорядження, рішення, накази або документи, розроблені в іншій формі, відповідно до вимог цього Положення; 4) затверджує механізми контролю та заходи з управління кіберризиками та ризиками інформаційної безпеки; 5) організовує підготовку та підвищення кваліфікації відповідальної особи за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту.	до 13.12.2026 (постійно)	
9	Забезпечення виконання вимог з інформаційної безпеки та кіберзахисту, що встановлені Положенням.	до 13.12.2026 (постійно)	
10	Розроблення внутрішніх документів з питань інформаційної безпеки відповідно до вимог Положення.	до 13.12.2026 (постійно)	
11	Організація регулярної актуалізації переліку / реєстру програмних та апаратних засобів інформаційно-комунікаційних систем Товариства.	до 13.12.2026 (постійно) / не рідше одного разу на рік з моменту останньої проведеної актуалізації	
12	Здійснення моніторингу та розслідування інцидентів інформаційної безпеки та кіберінцидентів.	до 13.12.2026 (постійно)	

13	Організація контролю за ефективністю функціонування засобів захисту інформації в інформаційно-комунікаційних системах Товариства та забезпечення відновлення їх працездатності в разі порушення штатного режиму функціонування.	до 13.12.2026 (постійно)	
14	Здійснення контролю за недопущенням встановлення та використання у складі інформаційно-комунікаційних систем програмних і апаратних засобів, не передбачених внутрішніми документами Товариства.	до 13.12.2026 (постійно)	
15	Погодження змін програмних та апаратних засобів інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем Товариства.	до 13.12.2026 (постійно)	
16	Забезпечення ознайомлення користувачів та привілейованих користувачів з внутрішніми документами Товариства з питань інформаційної безпеки та кіберзахисту під підпис або в інший спосіб, що забезпечує підтвердження ознайомлення.	до 13.12.2026 (постійно)	
17	Забезпечення перегляду внутрішніх документів з питань інформаційної безпеки та кіберзахисту та оновлення їх в разі суттєвої зміни умов функціонування інформаційно-комунікаційних систем, в яких Товариство під час надання послуг здійснює обробку інформації, яка віднесена до таємниці фінансової послуги.	Один раз на рік (з моменту останнього проведеного перегляду) / до 13.12.2026 (постійно)	
18	Забезпечення розподілу прав доступу до інформаційно-комунікаційних систем у спосіб, що дає змогу: 1) визначати права доступу клієнтів, користувачів та привілейованих користувачів до інформаційно-комунікаційних систем Товариства; 2) здійснити опис груп, ролей та розподіл повноважень клієнтів, користувачів та привілейованих користувачів інформаційно-комунікаційних систем (шаблони моделей доступу); 3) визначати права на виконання операцій (читання, модифікація, створення,	до 13.12.2026 (постійно)	

	видалення) для клієнтів, користувачів та привілейованих користувачів інформаційно-комунікаційних систем Товариства.		
19	Здійснення регулярного, але не рідше одного разу на рік з моменту останнього проведеного перегляду перегляд прав доступу клієнтів, користувачів та привілейованих користувачів до своїх інформаційно-комунікаційних систем.	до 13.12.2026 (постійно) / не рідше одного разу на рік з моменту останнього проведеного перегляду	
20	Забезпечення дотримання принципу надання мінімального рівня повноважень для користувачів та привілейованих користувачів, достатнього для виконання функціональних обов'язків під час надання доступу до інформаційно-комунікаційних систем.	до 13.12.2026 (постійно)	
21	Розроблення/актуалізація та затвердження внутрішніх документів, які встановлюють вимоги щодо управління правами доступу до інформаційно-комунікаційних систем Товариства і які повинні містити: 1) вимоги до ідентифікації, автентифікації, авторизації клієнтів, користувачів та привілейованих користувачів; 2) послідовність дій під час управління правами доступу; 3) порядок здійснення заходів контролю доступу; 4) вимоги до протоколювання дій під час управління правами доступу.	до 13.12.2026 (постійно)	
22	Запровадження технології та процедури автентифікації, які повинні впроваджуватися на основі внутрішніх документів, що регламентують контроль доступу для забезпечення автентифікації клієнтів, користувачів та привілейованих користувачів під час надання доступу до інформаційно-комунікаційних систем Товариства.	до 13.12.2026 (постійно)	
23	Організація та забезпечення доступу клієнтів, користувачів та привілейованих користувачів інформаційно-комунікаційних	до 13.12.2026 (постійно)	

	систем Товариства у межах встановлених для них прав доступу тільки після успішного проходження процедури автентифікації на підставі унікального персоніфікованого ідентифікатора (імені) клієнта, користувача, привілейованого користувача і пароля, що вводиться клієнтом, користувачем, привілейованим користувачем, або програмно-апаратного ідентифікатора (ключ, сертифікат, токен, біометрія).		
24	Запровадження та використання багатофакторної (множинної) автентифікації для користувачів та привілейованих користувачів під час здійснення ними віддаленого доступу до інформаційно-комунікаційних систем Товариства.	до 13.12.2026 (постійно)	
25	Забезпечення блокування / видалення облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах Товариства: 1) у разі кількох (до п’яти) невдалих спроб автентифікації поспіль (автоматичне тимчасове або постійне блокування); 2) якщо не було авторизації користувача, привілейованого користувача в інформаційно-комунікаційних системах Товариства протягом 90 календарних днів, − блокування на строк до авторизації особи користувача в безпечний доведений спосіб; 3) у разі звільнення користувача, привілейованого користувача або зміни статусу / функціональних обов’язків користувача, привілейованого користувача, який не передбачає доступу до цих систем; 4) у разі завершення дії договору з клієнтом.	до 13.12.2026 (постійно)	
26	Визначення та запровадження посилених вимог до паролів для облікових записів привілейованих користувачів (довжина та складність паролів, частота зміни) або застосування багатофакторної автентифікації для таких облікових записів. Привілейовані користувачі Товариства зобов’язані використовувати різні облікові записи для виконання функцій, які	до 13.12.2026 (постійно)	

	потребують привілейованих прав доступу, та повсякденних завдань. Користувачі зобов'язані використовувати складні паролі, які мають не менше ніж 12 символів та містять цифри, букви в різних регістрах та спеціальні символи (за умов, що система підтримує спеціальні символи). Привілейовані користувачі зобов'язані використовувати складні паролі, які мають не менше ніж 15 символів та містять цифри, букви в різних регістрах та спеціальні символи (за умов, що система підтримує спеціальні символи). Користувачі та привілейовані користувачі зобов'язані змінювати паролі в разі компрометації, але не рідше одного разу на 90 днів або в разі виявлення в базах скомпрометованих паролів. Повторення вибраного складного пароля може здійснюватися не раніше ніж на восьмий раз.		
27	Забезпечення: 1) можливості маскування значення пароля під час введення його клієнтом, користувачем та привілейованим користувачем; 2) блокування або перейменування облікових записів привілейованих користувачів інформаційно-комунікаційних систем та облікових записів користувачів операційних систем, що встановлюються за замовчуванням (за наявності технічної можливості та за умови збереження функціонування інформаційно-комунікаційних систем), та відключення гостьових облікових записів; 3) автоматичного блокування робочого столу 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);	до 13.12.2026 (постійно)	

	4) ідентифікації обладнання користувачів та привілейованих користувачів (персональні комп'ютери, мобільні пристрої), що підключається до інформаційно-комунікаційних систем Товариства (за апаратним ідентифікатором управління доступом до обладнання, сертифікатами, за допомогою спеціалізованого програмного забезпечення), та запровадження заходів, що унеможливлюють роботу обладнання в системах без відповідної ідентифікації.		
28	Забезпечення налаштування інформаційно-комунікаційних систем Товариства у спосіб, який забезпечує реєстрацію, збереження в журналах реєстрації подій (логи) та захист від модифікації інформації про такі події: 1) доступ до інформації з налаштуваннями програмного та апаратного забезпечення систем, журналів реєстрації подій (логи); 2) результати ідентифікації та автентифікації клієнтів, користувачів та привілейованих користувачів; 3) реєстрація подій, пов'язаних з управлінням правами доступу користувачів та привілейованих користувачів до інформаційно-комунікаційних систем та інформації, що циркулює в них; 4) авторизація / закриття сеансу роботи клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах; 5) невдалі спроби ідентифікації, автентифікації, авторизації клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах та перевищення граничної кількості спроб введення пароля; 6) реєстрація, видалення (блокування) облікових записів клієнтів, користувачів та привілейованих користувачів в інформаційно-комунікаційних системах; 7) зміна пароля клієнта, користувача та привілейованого користувача в інформаційно-комунікаційних системах;	до 13.12.2026 (постійно)	

	8) реєстрація подій, пов’язаних зі зміною конфігураційних налаштувань інформаційно-комунікаційних систем.		
29	Проведення періодичного архівування журналів реєстрації подій (логи) та забезпечення зберігання журналів реєстрації подій не менше одного року з моменту архівації, якщо інше не передбачено законодавством України.	до 13.12.2026 (постійно)/ не рідше одного разу на рік	
30	Забезпечення захисту журналів реєстрації подій (логи) та/або засобів ведення реєстрації цих подій від несанкціонованого доступу. Доступ до журналів реєстрації подій (логи) та/або засобів ведення реєстрації цих подій має надаватися тільки відповідальній особі.	до 13.12.2026 (постійно)	
31	Запровадження заходів забезпечення мережевого захисту, які повинні бути задокументовані у внутрішніх документах надавача фінансових послуг.	до 13.12.2026 (постійно)	
32	Здійснення розмежування інформаційно-комунікаційних систем на фізичному та/або логічному рівні (сегментацію мережі) і обмеження доступу між сегментами мережі з використанням міжмережевих екранів або аналогічних за функціональністю засобів мережевого захисту.	до 13.12.2026 (постійно)	
33	У разі підключення Товариством своїх інформаційно-комунікаційних систем до мережі Інтернет або зовнішніх мереж забезпечення виконання заходів мережевого захисту: 1) забезпечення взаємодії інформаційно-комунікаційних систем (її сегментів) із зовнішніми інформаційно-комунікаційними системами тільки через контрольовані точки доступу, кількість яких має бути мінімально необхідною для вирішення завдань; 2) встановлення заборони передачі інформації, що є об’єктом захисту, за межі інформаційно-комунікаційних систем у разі відмови (збою) функціонування засобів захисту; 3) переведення фізичних портів мережевого обладнання інформаційно-комунікаційних	до 13.12.2026 (постійно)	

	систем, які не використовуються, у стан «без призначення IPадреси»/«відключено» (за наявності технічної можливості реалізації); 4) забезпечення захисту від атак типу «відмова в обслуговуванні» та інших відомих мережевих атак.		
34	Забезпечення розміщення в зоні мережі з підвищеним рівнем безпеки інформаційно-комунікаційних систем Товариства, серверів та обладнання, що забезпечує функціонування сервісів (надання послуг), які відкриті для доступу клієнтів із зовнішніх мереж. Використання засобів захисту від шкідливого програмного коду з актуальними базами сигнатур.	до 13.12.2026 (постійно)	
35	Використання операційних систем, для яких діє підтримка з надання оновлень безпеки від виробника / розробника або постачальника 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.	до 13.12.2026 (постійно)	
36	Забезпечення блокування або перейменування облікових записів користувачів операційних систем, що встановлюються за замовчуванням, та відключення гостьових облікових записів.	до 13.12.2026 (постійно)	
37	Використання офіційних версій прикладного програмного забезпечення, для яких діє підтримка з надання оновлень безпеки від виробника / розробника або постачальника, та/або програмне забезпечення, розроблене для Товариства відповідно до укладених договорів постачання програмного забезпечення або розроблене самостійно Товариством.	до 13.12.2026 (постійно)	
38	Здійснення або організація здійснення підтримки прикладного програмного забезпечення, розробленого самостійно Товариством або розробленого для	до 13.12.2026 (постійно)	

	Товариства відповідно до укладених договорів постачання програмного забезпечення, включаючи оновлення безпеки, якщо інше не передбачено договором постачання програмного забезпечення.		
39	Проведення аналізу ризиків, пов'язаних з використанням програмного забезпечення, для якого припинено підтримку виробника / розробника або постачальника, та впровадження додаткових компенсуючих заходів, що включають: 1) упровадження додаткових заходів безпеки для захисту інформації (даних) та інформаційно-комунікаційних Товариства від потенційних загроз; 2) регулярний моніторинг та аудит інформаційної безпеки для виявлення та усунення вразливостей; 3) забезпечення резервного копіювання інформації (даних) та реалізації плану реагування на кіберінциденти та інциденти інформаційної безпеки з метою відновлення Товариства у разі настання таких інцидентів; 4) документування та затвердження результатів аналізу ризиків відповідно до внутрішніх документів з питань забезпечення інформаційної безпеки та кіберзахисту; 5) розробку плану переходу на офіційні версії прикладного програмного забезпечення, для яких діє підтримка з надання оновлень безпеки від виробника / розробника або постачальника.	до 13.12.2026 (постійно)	
40	Реалізація заходів, що визначені планом переходу на офіційні версії прикладного програмного забезпечення, для яких діє підтримка з надання оновлень безпеки від виробника / розробника або постачальника в строк, що не перевищує двох років, якщо інше не передбачено законом. План переходу на офіційні версії прикладного програмного забезпечення, для яких діє підтримка з надання оновлень безпеки від виробника / розробника або постачальника затверджується органом	до 13.12.2026 (постійно)	

	управління Товариства, відповідальним за здійснення нагляду за його діяльністю, та є складовою стратегії та/або плану діяльності, та/або плану безперервної діяльності Товариства, та/або іншого внутрішнього документа.		
41	Розроблення та затвердження внутрішніх документів, які встановлюють вимоги щодо безпеки інформації під час використання змінних носіїв інформації і повинні містити положення щодо: 1) контролю за використанням змінних носіїв інформації, включаючи процедури їх обліку та виведення з експлуатації; 2) категорії інформації, яка може оброблятися на змінних носіях інформації; 3) обов'язкової ідентифікації змінних носіїв інформації, які використовуються Товариством за допомогою унікального ідентифікатора, який дає змогу визначити тип носія та користувача змінного носія; 4) обмежень використання змінних носіїв інформації; 5) знищення інформації на змінних носіях інформації перед їх передаванням у користування іншому працівникові Товариства, третім особам або виведенням з експлуатації; 6) обов'язкової перевірки змінних носіїв інформації на наявність шкідливого програмного забезпечення перед використанням Товариством.	до 13.12.2026 (постійно)	
42	Здійснення ідентифікації змінних носіїв інформації за допомогою унікального ідентифікатора, який дасть змогу визначити тип носія та користувача змінного носія.	до 13.12.2026 (постійно)	
43	Упровадження процесу управління кіберінцидентами та інцидентами інформаційної безпеки, розроблення і затвердження плану реагування на кіберінциденти та інциденти інформаційної безпеки. Планування реагування на кіберінциденти та інциденти інформаційної безпеки є частиною планування на випадок надзвичайних ситуацій для Товариства і має	до 13.12.2026 (постійно)	

	розглядатися в сукупності із реагуванням на інші інциденти безпеки.		
44	План реагування на кіберінциденти та інциденти інформаційної безпеки повинен бути розроблений з урахуванням внутрішніх документів з питань забезпечення безперервності діяльності або бути складовою плану безперервної діяльності Товариства та містити: 1) оцінки негативного впливу (збитку), нанесеного Товариству кіберінцидентом та інцидентом інформаційної безпеки; 2) порядок дій відповідальної особи за забезпечення впровадження вимог з інформаційної безпеки та кіберзахисту під час реагування на кіберінциденти та інциденти інформаційної безпеки; 3) описи дій користувачів та привілейованих користувачів у разі впровадження кіберінцидентів та інцидентів інформаційної безпеки; 4) порядок взаємодії відповідальної особи за забезпечення виконання вимог з інформаційної безпеки та кіберзахисту з працівниками основних бізнес-процесів Товариства під час реагування на кіберінциденти та інциденти інформаційної безпеки; 5) порядок інформування Директора Товариства про кіберінциденти та інциденти інформаційної безпеки; 6) описи дій зі зберігання інформації щодо кіберінцидентів та інцидентів інформаційної безпеки, їх аналізу та результатів реагування.	до 13.12.2026 (постійно)	
45	Забезпечення взаємодії з особами, які залучаються для виконання заходів із забезпечення інформаційної безпеки та з реагування на інциденти інформаційної безпеки та інциденти кібербезпеки, включаючи розробників програмного забезпечення, системних інтеграторів, компанії, що забезпечують технічну підтримку інформаційно-комунікаційних систем.	до 13.12.2026 (постійно)	

46	Здійснення моніторингу подій під час дії договору з особами, які залучаються для виконання заходів із забезпечення інформаційної безпеки, зокрема кіберінцидентів, інцидентів інформаційної безпеки, інцидентів порушення безперервності діяльності, що впливають (можуть вплинути) на надання послуг.	до 13.12.2026 (постійно)	
47	Переглянути Посадову інструкцію фахівця із інформаційної безпеки та інших працівників з урахуванням вимог Положення та у разі необхідності внести до них зміни.	до 13.12.2026 (постійно)	