

ЧЕК-ЛИСТ ДЛЯ ІТ-, ІБ- ТА РИЗИК-КОМАНД

Чи готова ваша організація до вимог НБУ?

Спрощений чек-лист попередньої самоперевірки інформаційної безпеки та кіберзахисту

22

простих запитання

5

ключових блоків

10 хв

на проходження

Так / Частково / Ні

без складних розрахунків

Для банків, страхових компаній, кредитних спілок, фінансових компаній, ломбардів та команд, які проводять внутрішню оцінку готовності.

Матеріал підготовлено на основі офіційних документів НБУ. Запитання викладено простою мовою і не є офіційною формою регулятора.

Як користуватися чек-листом?

Пройдіть 22 запитання та позначте фактичний стан на сьогодні.

Так

Процес працює, відповідальний визначений, а підтвердження можна показати.

Частково

Щось уже зроблено, але є прогалини, застарілі документи або неповне охоплення.

Ні

Процесу немає або команда не може підтвердити, що він реально працює.

Важливо

Точний перелік вимог залежить від типу установи, її послуг, статусу та належності до критичної інфраструктури. Цей матеріал допомагає підготуватися до внутрішньої оцінки, але не замінює аудит, юридичний висновок або офіційне роз'яснення НБУ.

На що звернути увагу в першу чергу

- чи є відповідальний за інформаційну безпеку та кіберзахист;
- чи відомі всі критичні та доступні з Інтернету активи;
- чи виявляються та усуваються вразливості;
- чи контролюються привілейовані й віддалені доступи;
- чи є план реагування та перевірене відновлення з резервних копій.

Офіційна основа

Для банків Постанова НБУ №4 передбачає щорічну самооцінку стану інформаційної безпеки/кіберзахисту. Для надавачів небанківських фінансових послуг Постанова №143 визначає вимоги до управління ризиками, організації захисту, доступу та реагування на інциденти.

1. ВІДПОВІДАЛЬНІСТЬ, ДОКУМЕНТИ ТА РИЗИКИ

Перевірте, чи зрозуміло, хто відповідає за захист і як керівництво контролює ризики.

№	Що перевірити	Відповідь
1	Визначено відповідальну особу або команду за інформаційну безпеку та кіберзахист. Підтвердження: наказ, посадова інструкція, організаційна структура	☐ Так ☐ Частково ☐ Ні
2	Ролі, повноваження та порядок взаємодії між IT, ІБ, ризиками й керівництвом описані та актуальні. Підтвердження: внутрішні документи, розподіл відповідальності	☐ Так ☐ Частково ☐ Ні
3	Ризики інформаційної безпеки та кіберризики регулярно оцінюються, а важливі результати розглядає керівництво. Підтвердження: реєстр ризиків, звіт, протокол або рішення	☐ Так ☐ Частково ☐ Ні
4	Основні політики й процедури затверджені, переглядаються та відповідають фактичній роботі команди. Підтвердження: актуальні версії документів, дати перегляду	☐ Так ☐ Частково ☐ Ні

Практична порада SOFTICO

Попросіть відповідального показати останній перелік головних кіберризиків і рішення керівництва щодо них. Якщо такого переліку немає, почніть саме з нього.

Нормативна основа

Для банків: Постанови НБУ №95, №4 і №178. Для небанківських надавачів фінансових послуг: Постанова №143.

2. АКТИВИ, ВРАЗЛИВОСТІ ТА ОНОВЛЕННЯ

Організація має розуміти, що саме вона захищає і які слабкі місця потребують першочергового усунення.

№	Що перевірити	Відповідь
5	Є актуальний перелік серверів, робочих станцій, мережевого обладнання, хмарних ресурсів, вебсервісів та інших важливих активів. Підтвердження: реєстр активів або автоматичний звіт виявлення	☐ Так ☐ Частково ☐ Ні
6	Критичні для бізнесу та доступні з Інтернету активи чітко позначені. Підтвердження: класифікація активів, схема або список зовнішніх ресурсів	☐ Так ☐ Частково ☐ Ні
7	Системи регулярно перевіряються на вразливості та небезпечні налаштування. Підтвердження: актуальні звіти перевірок і графік сканувань	☐ Так ☐ Частково ☐ Ні
8	Для знайдених проблем визначені пріоритет, відповідальний і строк усунення. Підтвердження: задачі, реєстр вразливостей, погоджені винятки	☐ Так ☐ Частково ☐ Ні
9	Після виправлення проводиться повторна перевірка, щоб підтвердити результат. Підтвердження: повторне сканування або підтвердження закриття	☐ Так ☐ Частково ☐ Ні

Практична порада SOFTICO

Не намагайтеся виправити все одночасно. Спочатку перевірте критичні системи, інтернет-доступні ресурси та вразливості, які реально можуть бути використані.

Нормативна основа

Постанова №178 передбачає заходи протидії кіберзагрозам з урахуванням аналізу вразливостей. Постанова №143 містить вимоги щодо моніторингу та усунення вразливостей, зокрема для ПЗ без підтримки.

3. ДОСТУПИ ТА ОБЛІКОВІ ЗАПИСИ

Надмірні або неконтрольовані права доступу є однією з найнебезпечніших прогалин.

№	Що перевірити	Відповідь
10	Користувачі отримують лише ті права, які потрібні для виконання їхніх обов'язків. Підтвердження: правила доступу, ролі, заявки на надання прав	☐ Так ☐ Частково ☐ Ні
11	Права доступу регулярно переглядаються та швидко змінюються після переведення або звільнення працівника. Підтвердження: результати перегляду, вибірка закритих облікових записів	☐ Так ☐ Частково ☐ Ні
12	Для віддаленого та привілейованого доступу використовується багатофакторна автентифікація. Підтвердження: налаштування MFA, перелік винятків	☐ Так ☐ Частково ☐ Ні
13	Дії адміністраторів і зміни прав доступу реєструються та можуть бути перевірені. Підтвердження: журнали подій, звіт про адміністративні дії	☐ Так ☐ Частково ☐ Ні

Практична порада SOFTICO

Створіть один список усіх адміністраторських і віддалених облікових записів. Для кожного перевірте власника, необхідність доступу, MFA та дату останнього перегляду.

Нормативна основа

Постанова №143 прямо визначає вимоги до управління правами доступу, мінімальних повноважень, автентифікації, MFA для віддаленого доступу та протоколювання дій.

4. МОНІТОРИНГ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ

Важливо не лише встановити засоби захисту, а й уміти вчасно помітити подію та організовано відреагувати.

№	Що перевірити	Відповідь
14	Події безпеки з важливих систем збираються, зберігаються та регулярно переглядаються. Підтвердження: перелік джерел логів, звіти або панель моніторингу	☐ Так ☐ Частково ☐ Ні
15	Є затверджений і зрозумілий план реагування на кіберінциденти та інциденти інформаційної безпеки. Підтвердження: план реагування, контакти, порядок ескалації	☐ Так ☐ Частково ☐ Ні
16	Працівники знають, куди повідомляти про фішинг, підозрілу активність, втрату пристрою чи іншу подію. Підтвердження: інструкція, канал повідомлення, навчальні матеріали	☐ Так ☐ Частково ☐ Ні
17	План реагування перевірявся на практиці або під час навчальної вправи, а недоліки були зафіксовані. Підтвердження: звіт про вправу, перелік коригувальних дій	☐ Так ☐ Частково ☐ Ні

Практична порада SOFTICO

Проведіть коротку настільну вправу: “скомпрометовано обліковий запис адміністратора”. Перевірте, чи команда знає перші дії, контакти та порядок інформування керівництва.

Нормативна основа

Постанова №143 вимагає впровадити процес управління інцидентами та затвердити план реагування. Постанова №178 регулює організацію кіберзахисту банків і взаємодію щодо кіберзагроз та кіберінцидентів.

5. ВІДНОВЛЕННЯ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА ПОСТАЧАЛЬНИКИ

Останній блок показує, чи може організація продовжити роботу після збою або кібератаки.

№	Що перевірити	Відповідь
18	Критичні дані та конфігурації регулярно резервуються, а доступ до резервних копій контролюється. Підтвердження: звіт резервного копіювання, перелік охоплених систем	☐ Так ☐ Частково ☐ Ні
19	Відновлення з резервних копій перевірялося на практиці, а результат задокументований. Підтвердження: звіт тестового відновлення, виявлені проблеми	☐ Так ☐ Частково ☐ Ні
20	Відомо, де використовується програмне забезпечення без підтримки або без актуальних оновлень безпеки. Підтвердження: перелік такого ПЗ, аналіз ризику, план заміни	☐ Так ☐ Частково ☐ Ні
21	Ризики постачальників і хмарних сервісів, які мають доступ до систем або даних, оцінюються та контролюються. Підтвердження: реєстр постачальників, вимоги безпеки, відповідальні контакти	☐ Так ☐ Частково ☐ Ні
22	Документи й технічні підтвердження зібрані так, щоб їх можна було швидко знайти під час внутрішньої оцінки або перевірки. Підтвердження: структурована папка або реєстр доказів	☐ Так ☐ Частково ☐ Ні

Практична порада SOFTICO

Не обмежуйтеся питанням “чи є резервна копія?”. Запитайте: “коли востаннє ми реально відновили критичну систему і що не спрацювало?”.

Нормативна основа

Постанова №143 містить вимоги щодо ризиків ПЗ без підтримки, резервного копіювання та планування відновлення. Для банків відповідні заходи визначаються нормативними актами НБУ з інформаційної безпеки та кіберзахисту.

Як оцінити результат?

Не потрібно рахувати складний бал.
Подивіться на відповіді “Ні” та “Частково”.

Зелена зона	Більшість відповідей “Так”, а в критичних питаннях немає “Ні”. Проведіть фінальну перевірку документів і застосовності вимог.
Жовта зона	Є кілька відповідей “Частково” або “Ні”. Складіть короткий план: дія, відповідальний, строк, підтвердження результату.
Червона зона	Є “Ні” у критичних питаннях нижче. Спочатку закрийте ці прогалини, навіть якщо загальна картина виглядає непогано.

Критичні запитання

- 1 — відповідальний за інформаційну безпеку та кіберзахист;
- 5 — актуальний перелік активів;
- 7 — регулярне виявлення вразливостей;
- 10 і 12 — контроль прав та MFA;
- 15 — план реагування на інциденти;
- 18 і 19 — план реагування на інциденти;

Орієнтовна інтерпретація

Це практична методика SOFTICO, а не офіційна шкала НБУ. Вона допомагає визначити пріоритети, але не підтверджує відповідність установи нормативним вимогам.

5 перших кроків після чек-листа

01

Призначте власника кожної прогалини

У кожної відповіді “Ні” або “Частково” має бути конкретний відповідальний.

02

Складіть короткий перелік критичних активів

Почніть із систем, від яких залежить надання послуг, і ресурсів, доступних з Інтернету.

03

Перевірте зовнішню поверхню атаки та вразливості

Знайдіть невідомі активи, небезпечні налаштування, застаріле ПЗ та критичні вразливості.

04

Перегляньте адміністраторські та віддалені доступи

Приберіть зайві права, увімкніть MFA, закрийте невикористовувані облікові записи.

05

Перевірте відновлення та план реагування

Проведіть тест відновлення і коротку вправу з реагування на інцидент.

Формат плану

Прогалина



Ризик



Дія



Відповідальний



Строк



Доказ виконання

Такий формат простий, зрозумілий керівництву й допомагає контролювати реальний прогрес.

Де може допомогти Holm Security?

Платформа може підтримати технічну частину управління вразливостями та підготовку доказів.

Можливість	Практична користь
Виявлення активів	Допомагає автоматично знаходити та відстежувати системи, вебресурси, домени, хмарні й локальні активи.
Пошук вразливостей	Проводить оцінювання систем, мереж, вебзастосунків та інших підтримуваних типів активів.
Пріоритизація	Допомагає визначити, які вразливості варто усунути першими з урахуванням ризику та впливу активу.
Контроль усунення	Підтримує роботу від виявлення проблеми до повторної перевірки та звітності.

Що рішення не замінює

Holm Security не замінює управлінські рішення, внутрішні політики, управління доступом, резервне копіювання, план реагування, аудит або юридичну оцінку відповідності. Коректне формулювання: рішення допомагає підтримати виконання окремих технічних і процесних вимог.

Офіційні джерела

- НБУ, Постанова №95 від 28.09.2017
- НБУ, Постанова №4 від 16.01.2021
- НБУ, Постанова №178 від 12.08.2022
- НБУ, Постанова №143 від 09.12.2025

- НБУ, Постанова №66 від 12.06.2026 — для критичної інформаційної інфраструктури фінансового сектору
- Holm Security, Vulnerability Management
- Holm Security, Attack Surface Management

Потрібно оцінити покриття активів і систематизувати управління вразливостями?

Команда SOFTICO допоможе провести демонстрацію Holm Security та спланувати пілотний проєкт.