Додаток № 1
до Наказу № 1040 від 30.06.2023

ПОЛІТИКА
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
ТОВ «НоваПей»

(редакція **8.0)**

Київ

Загальна інформація про документ:

Розробник документу:	Відділ інформаційної безпеки
Посада та ПІБ виконавця, відповідального за розробку:	Начальник Відділу інформаційної безпеки Сніжко Д.М.
Власник процесу	Відділ інформаційної безпеки
Дія документа поширюється на:	Усі структурні підрозділи та Філії Товариства
Рівень доступу	Доступ: загальний

Історія документа:

Редакція №	**Дата і номер документа про затвердження**	**Дія**
1.0	*Наказ Генерального Директора №527 від 16.01.2017*	*Затверджена версія 1.0.*
2.0	*Наказ Генерального Директора №330 від 26.03.2018*	*Затверджена версія 2.0*
3.0	*Наказ Генерального Директора №569 від 28.05.2019*	*Затверджена версія 3.0*
4.0	*Наказ Генерального Директора №348 від10.03.2020*	*Затверджена версія 4.0*
5.0	*Наказ Генерального Директора №1324 від 16.11.2020*	*Затверджена версія 5.0*
6.0	*Наказ Генерального директора №373 від 02.04.2021 року*	*Затверджена версія 6.0*
7.0	*Наказ Генерального директора №218 від 13.02.2023 року*	*Затверджена версія 7.0*
8.0	*Наказ Генерального директора № 1040 від 30.06.2023 року*	*Затверджена версія 8.0*

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Політика інформаційної безпеки ТОВ «НоваПей» (далі – Політика) визначає загальні вимоги до організації інформаційної безпеки у ТОВ «НоваПей», основні принципи, цілі та завдання системи управління інформаційною безпекою ТОВ «НоваПей» (далі – Товариство).

1.2. Забезпечення інформаційної безпеки є невід'ємною частиною діяльності Товариства. Стан захищеності являє собою вміння та здатність Товариства надійно протистояти будь-яким спробам завдати шкоди його законним інтересам.

1.3. Керівництво Товариства усвідомлює важливість та необхідність вдосконалення заходів і засобів забезпечення інформаційної безпеки в контексті розвитку законодавства та норм регулювання діяльності, а також розвитку реалізованих технологій та очікувань клієнтів Товариства та інших зацікавлених сторін.

1.4. Перелік зацікавлених сторін та їх вимог до системи управління інформаційною безпекою (далі – СУІБ) наведений у Додатку 1 до цієї Політики.

1.5. Під час розробки Політики використовувалися наступні документи:

- Цивільний кодекс України;
- Кодекс законів про працю України;
- Закон України «Про інформацію»;
- Закон України «Про доступ до публічної інформації»;
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Закон України «Про платіжні послуги»;
- Закон України «Про захист персональних даних»;
- ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги;
- ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT);
- Стандарт безпеки даних індустрії платіжних карток PCI DSS.

1.6. Політика інформаційної безпеки Товариства складається з цієї Політики та іншої внутрішньої документації СУІБ Товариства.

1.7. Терміни та скорочення, які використовуються у цій Політиці та документації СУІБ Товариства, наведені у Додатку 2 до цієї Політики.

1.8. Політика поширюється на всі підрозділи Товариства та обов’язкова до застосування кожним працівником Товариства.

1.9. Політика може бути опублікована на офіційному сайті Товариства та надаватись третім сторонам в рамках контрактних або партнерських зобов'язань Товариства.

2. ЦІЛЬ ДОКУМЕНТА

2.1. Ціллю Політики є впровадження та ефективне функціонування СУІБ, яка буде:

2.1.1. відповідати вимогам: стратегії Товариства, законодавства, контрактних та партнерських зобов’язань перед третіми сторонами;

2.1.2. забезпечувати захист інформації та ресурсів Товариства від зовнішніх і внутрішніх загроз, у тому числі загроз, які пов’язані з розголошенням, втратою, витоком, спотворенням та/або знищенням інформації, що становить комерційну таємницю, персональні дані та іншу конфіденційну інформацію;

2.1.3. забезпечувати захист інформації , кіберзахисту та інформаційної безпеки, під час надання платіжних послуг клієнтам;

2.1.4. сприяти мінімізації ризиків операційної діяльності Товариства;

2.1.5. забезпечувати цілісність, конфіденційність, доступність та спостережність інформації в Товаристві;
2.1.6. створювати позитивну репутацію Товариства при роботі з клієнтами, партнерами і постачальниками послуг.

3. СФЕРА ЗАСТОСУВАННЯ

3.1. Політика розповсюджується на всі структурні підрозділи Товариства та повинна використовуватися для усіх процесів Товариства. Зокрема, вимоги інформаційної безпеки враховуються та виконуються:
3.1.1. при обробці інформації у будь-якому вигляді (на паперових або електронних носіях, вербальної тощо);
3.1.2. при забезпеченні життєдіяльності Товариства (управління персоналом, охорона приміщень, управління системами життєзабезпечення тощо);
3.1.3. при управлінні інформаційно-телекомунікаційною системою Товариства;
3.1.4. при управлінні безперервністю бізнесу;
3.1.5. при наданні платіжних послу клієнтам;
3.1.6. при взаємодії з третіми сторонами;
3.1.7. при розробці нових продуктів та впровадженні інформаційних систем.

4. ОРГАНІЗАЦІЙНА СТРУКТУРА ПРОЦЕСУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

4.1. При побудові та функціонуванні СУІБ Товариство використовує ризик-орієнтовний підхід, який забезпечує управління інцидентами інформаційної безпеки, визначення цілей заходів безпеки та їх ефективне використання. Деталі ризик-орієнтовного підходу описані в Політиці управління інформаційною безпекою.
4.2. У Товаристві впроваджена трирівнева модель управління ризиками інформаційної безпеки і кіберризиками з розподілом обов'язків між підрозділами відповідно до наступного:
- перша лінія - бізнес-підрозділи та підрозділи підтримки, які є власниками всіх операційних ризиків, що виникають у сфері їх відповідальності;
- друга лінія - Департамент управління ризиками, що координує в цілому систему управління операційним ризиком, Дирекція з комплаєнс контролю, яка забезпечує контроль дотриманням норм законодавства, та внутрішніх положень Товариства;
- третя лінія захисту - внутрішній аудит, який здійснює оцінку ефективності системи управління операційним ризиком підрозділами першого та другого рівнів захисту, включаючи оцінку ефективності системи внутрішнього контролю.

4.3. Відповідно до організаційної структури системи управління ризиками - підрозділ інформаційної безпеки відноситься до першої лінії захисту. В рамках системи управління ризиками підрозділ з інформаційної безпеки несе відповідальність за ризики ІБ та звітує Генеральному директору Товариства щодо поточного стану управління такими ризиками та системи управління інформаційною безпекою в цілому.

5. ПІДХОДИ ЩОДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

5.1. Підходи до визначення цілей СУІБ

Для підтримання належного захисту інформації (насамперед інформації з обмеженим доступом) із забезпеченням її цілісності, конфіденційності, доступності та спостережності визначаються цілі інформаційної безпеки. Цілі інформаційної безпеки виражаються у вигляді характеристик і параметрів, для досягнення яких впроваджуються заходи інформаційної

безпеки, та встановлюються якісні та кількісні показники в системі внутрішнього контролю процесів СУІБ.

Джерелами для формування цілей інформаційної безпеки є зовнішні та внутрішні фактори, що визначають діяльність Товариства, а саме:

- закони України;
- стандарти інформаційної безпеки;
- нормативно-правові акти Національного банку України;
- правила платіжних систем та систем переказу коштів;
- угоди з третіми сторонами;
- результати оцінки ризиків, які враховують загальну бізнес-стратегію та цілі діяльності Товариства;
- внутрішні нормативні документи Товариства, що регламентують принципи обміну та обробки інформації відповідно до бізнес-потреб.

5.2. Управління ризиками інформаційної безпеки

При управлінні ризиками інформаційної безпеки Товариство керується основними принципами системи управління ризиком в Товаристві:

- дотримання трирівневої моделі управління ризиками;
- створення та впровадження процедури управління ризиком інформаційної безпеки з метою ефективного управління ризиком інформаційної безпеки/кіберризиком;
- забезпечення своєчасного виявлення загроз інформаційної безпеки та усунення ризиків інформаційної безпеки;
- виявлення і врахування факторів ризику, які загрожують доступності, цілісності, конфіденційності інформації в Товаристві.
- забезпечення обізнаності працівників Товариства щодо ризиків інформаційної безпеки.

5.3. Управління інцидентами інформаційної безпеки складається з:

- виявлення і фіксації подій ІБ найбільш ефективним шляхом, підтвердження їх класифікації як інцидентів ІБ;
- послідовна оцінка та безперервне реагування на виявлені інциденти ІБ найбільш сприятливим та ефективним чином;
- застосування ефективної системи управління інцидентами, для зведення до мінімуму несприятливих наслідків для Товариства;
- використання своєчасного інформування відповідальних осіб за інформаційну безпеку про інциденти ІБ, за допомогою процесу ескалації;
- впровадження моніторингу, оцінки та усунення вразливостей ІБ, для скорочення кількості інцидентів;
- швидке вилучення досвіду за результатами управління інцидентами ІБ та застосування його в майбутньому для запобігання таких інцидентів ІБ.

6. ПРИНЦИПИ ТА ВИМОГИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

6.1. Основним принципом Політики є підтримання належного та визначеного рівня захисту інформації із забезпеченням її цілісності, конфіденційності, доступності та спостережності.

6.2. Принципами забезпечення інформаційної безпеки є:

- системний (комплексний) підхід до забезпечення інформаційної безпеки Товариства;
- безперервність процесу удосконалення та розвитку інформаційної безпеки та його
- здійснення шляхом обґрунтування та реалізації раціональних засобів, методів, заходів із застосуванням найкращого міжнародного досвіду;

— своєчасність та адекватність заходів захисту від реальних та потенційних загроз інформаційній безпеці Товариству;
— контроль та забезпечення підтримки належного рівня інформаційної безпеки з боку
— керівників Товариства;
— забезпечення достатності ресурсів, у тому числі фінансових, для сталого розвитку
— систем інформаційної безпеки Товариства.

6.3. Керівництво Товариство всіляко підтримує впровадження інформаційної безпеки та забезпечує її фінансування на достатньому рівні.
6.4. У Товаристві діє принцип надання мінімального рівня повноважень під час надання доступу до інформаційних систем Товариства (включаючи доступ привілейованих користувачів).
6.5. Під час розроблення, впровадження та функціонування програмно-технічних комплексів обов'язково враховуються вимоги інформаційної безпеки.
6.6. Внутрішні мережі Товариства мають відповідати вимогам стандартів з інформаційної безпеки.
6.7. Товариство забезпечує виконання вимог з інформаційної безпеки, які наявні в угодах з третіми сторонами стосовно участі у міжнародних платіжних системах та системах переказу коштів.
6.8. Кожен працівник Товариства під час виконання своїх посадових обов'язків і повноважень повинен забезпечувати виконання вимог інформаційної безпеки Товариства.
6.9. Працівники Товариства несуть відповідальність за невиконання вимог інформаційної безпеки, встановлених внутрішніми документами Товариства та нормами чинного законодавства.
6.10. Вимоги Політики, за необхідності, доводяться до відома представникам третіх сторін.
6.11. Товариство зобов'язане ознайомити з Політикою працівників під час прийому на роботу під підпис та отримати зобов'язання про дотримання конфіденційності.

7. СИСТЕМА ВНУТРІШНЬОГО КОНТРОЛЮ

7.1. Керівництво Товариства чітко розуміє, що інформаційна безпека Товариства є основою життєдіяльності Товариства.
7.2. Керівництво Товариства формулює принципи та завдання інформаційної безпеки.
7.3. Керівництво Товариства сприяє створенню, впровадженню, контролю, підтримці та вдосконаленню політики інформаційної безпеки.
7.4. Документи СУІБ Товариства розробляються Відділом ІБ та іншими підрозділами за відповідними напрямками діяльності.
7.5. Вимоги інформаційної безпеки затверджуються Генеральним директором Товариства, рішення якого є обов’язковими для виконання усім персоналом Товариства.
7.6. Постійний контроль впровадження, виконання, вдосконалення та підтримка Політики в актуальному стані покладено на Відділ ІБ.
7.7. Функціонально пов’язані структурні підрозділи Товариства, що приймають участь в розробці та узгоджені документів несуть відповідальність за зміст та актуальність документів СУІБ в межах своєї компетенції.
7.8. Керівництво Товариства створює умови для систематичного навчання працівників Товариства вимогам та заходам інформаційної безпеки. Систематичне навчання персоналу Товариства з питань інформаційної безпеки проводить Відділ ІБ із залученням Управління організації операційної роботи і навчання персоналу мережі Дирекції персоналу та адміністративних питань.
7.9. Кожен працівник Товариства у межах своїх повноважень забезпечує підтримку відповідного рівня інформаційної безпеки Товариства, в тому числі виконання вимог

документів СУІБ, законодавчих та регуляторних норм та несе відповідальність за їх порушення згідно із законодавством України і внутрішніми нормативними документами.

7.10. Документи СУІБ доступні працівникам Товариства у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки.

8. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

8.1. Політика вступає в силу з дати її затвердження наказом Генерального директора Товариства.

8.2. Ця Політика охоплює наступні заходи захисту Стандартів:
ДСТУ ISO/IEC 27001:2015 “Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги”:
- A.5.1 Принципи управління інформаційною безпекою;

Стандарт безпеки даних індустрії платіжних карт (PCI DSS), версія 4.0 “Вимоги та процедури оцінки безпеки”:
- Вимога 12.1 Розробити, опублікувати, підтримувати і поширювати політику інформаційної безпеки.

8.3. Зміни та доповнення до цієї Політики затверджуються наказом Генерального директора Товариства та можуть оформлятися, в тому числі, шляхом викладення Політики в новій редакції.

8.4. У разі невідповідності будь-якої частини цієї Політики чинному законодавству України, в тому числі в зв'язку з прийняттям нових нормативно-правових актів, Політика діятиме тільки в тій частині, яка не суперечить чинному законодавству України.

8.5. Надання Політики зовнішнім органам, третім особам відбувається за обов’язковим погодженням з Департаментом інформаційних технологій та Відділом інформаційної безпеки відповідно до діючого законодавства України.

8.6. У разі необхідності ця Політика переглядається із метою поліпшення ефективності бізнес-процесів Товариства та удосконалення системи внутрішнього контролю, але не рідше ніж раз на рік.

8.7. У разі зміни назв структурних підрозділів, які задіяні в процедурах, що описані у цій Політиці, при незмінності функцій, ця Політика вважається дійсною щодо їх нової назви.

Додаток 1

Зацікавлені сторони, пов’язані з СУІБ

№ п/п	Зацікавлені сторони	Вимоги та очікування зацікавлених сторін
1.	Власники Товариства	- виконання вимог законодавства України; - забезпечення захисту активів, у тому числі персоналу та інформації; - мінімізація ризиків інформаційної безпеки.
2.	Персонал	- забезпечення захисту персональних даних; - забезпечення особистої безпеки на робочому місці; - забезпечення захисту активів, з якими працює персонал.
3.	Клієнти	- забезпечення якісного, безперервного та безпечного отримання послуг згідно контрактних угод; - захист інформації при наданні платіжних послуг; - захист активів (коштів); - захист інформації: комерційної таємниці та персональних даних.
4.	Регулятори	- виконання вимог законодавства України; - забезпечення кіберстійкості та безперервності діяльності платіжної інфраструктури на належному рівні; - виконання ліцензійних умов; - виконання вимог безпеки, зафіксованих в угодах.
5.	Партнери, контрагенти – постачальники послуг	- забезпечення якісного, безперервного та безпечного надання послуг згідно контрактних угод; - захист інформації: комерційної таємниці та персональних даних; - виконання вимог безпеки, зафіксованих в угодах.

Додаток 2

Терміни та скорочення, які використовуються в документації СУІБ

1. **Автентифікація** (authentification) – забезпечення гарантії того, що характеристики об’єкта, які було заявлено, є правильними.
2. **Автентичність** (authenticity) – властивість, що об'єкт саме той, яким себе заявляє.
3. **Авторизація** (authorization) – надання об’єкту визначених повноважень, після проведення його ідентифікації та автентифікації.
4. **Верифікація –** підтвердження наданням об’єктивних доказів, що встановлені вимоги виконано.
5. **Виток інформації –** результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї.
6. **Відстежуваність –** властивість інформації або ресурсу, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки та/або забезпечення відповідальності за певні дії.
7. **Власник ресурсу** – посадова особа Товариства, якій надано повноваження та встановлено відповідальність за прийняття рішення щодо надання доступу до ресурсу (інформації, яка обробляється у ресурсі). Власник ресурсу разом із Відділом інформаційної безпеки визначає вимоги безпеки ресурсу з урахуванням вимог законодавства та загальної політики безпеки Товариства.
8. **Вразливість** – слабкість ресурсу або заходів безпеки, якою можуть скористатися одна чи більше загроз.
9. **Відділ ІБ (ВІБ)** – Відділ інформаційної безпеки Товариства.
10. **Департамент ІТ (ДІТ) –** Департамент інформаційних технологій Товариства.
11. **Доступність** – властивість досяжності й можливості використання на вимогу об’єкта, який має повноваження та пройшов авторизацію.
12. **Електронний носій інформації** – всі цифрові та магнітні носії інформації, призначені для запису, зберігання та зчитування інформації, яка представлена в цифровому коді (USB – накопичувачі, карти пам’яті, оптичні диски, зовнішні та внутрішні жорсткі диски).
13. **Загроза** – потенційна причина небажаного інциденту, який може спричинити шкоду для системи або Товариства.
14. **Зацікавлені сторони** – фізична або юридична особа(и), яка може впливати на прийняття будь-якого рішення чи дії, підпадати під його вплив або відчувати можливість такого впливу.
15. **Засоби захисту інформації** – програмно-технічні засоби, які забезпечують захист електронних документів від несанкціонованих дій щодо ознайомлення з їх змістом, модифікації або викривлення на етапі їх передавання або зберігання.
16. **Захист інформації** – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.
17. **Ідентифікація** (identification) – процедура розпізнавання об’єкта на підставі наданих характеристик.
18. **Інформаційна безпека** – забезпечення визначеного рівня основних властивостей інформації: конфіденційності, цілісності, доступності інформації.
    В залежності від ризиків можна додатково розглядати інші властивості, такі як автентичність, відстежуваність, неспростовність та надійність.
19. **Інформаційна система/Інформаційно-телекомунікаційна система (ІС/ІТС)** – сукупність інформаційних та телекомунікаційних систем, які в процесі обробки інформації діють як одне ціле.
20. **Інформація -** будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді чи передані вербально.
21. **Інцидент інформаційної безпеки** – одна подія чи серія небажаних та/або непередбачуваних подій порушення ІБ, які можуть призвести до збитків та втрат для суб’єкта інформаційного захисту або користувачів ІС. Впливає на інформаційну безпеку ІС та ІТ мережі.
22. **Кібербезпека, кіберзахищеність** – стан упевненості в захисті від фізичного, фінансового чи іншого наслідків несправностей, пошкоджень, помилок, збитків чи інших подій у кіберпросторі,

які можна вважати небажаними. Своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз ІБ у кіберпросторі.

23. **Керівництво Товариства (Керівництво)** – керівна ланка Товариства від Генерального директора до керівників департаментів (включно), які формують стратегію розвитку Товариства, в тому числі і в напрямку інформаційної безпеки.
24. **Кіберінцидент –** подія або сукупність несприятливих подій ненавмисного характеру, або таких, що мають ознаки можливої кібератаки, які становлять загрозу безпеці інформаційної інфраструктури, створюють імовірність порушення штатного режиму її функціонування, а також ставлять під загрозу захищеність інформаційних ресурсів. Кіберінцидент є видом інцидентів інформаційної безпеки
25. **Кіберзагроза -** наявні та потенційно можливі явища і чинники, що спричиняють або можуть спричинити ризик порушення конфіденційності, цілісності, доступності інформаційних ресурсів та/або спостережності і керованості інформаційної інфраструктури.
26. **Кіберстійкість платіжної системи –** спроможність платіжної організації, учасників платіжної системи, операторів послуг платіжної інфраструктури та розрахункового(их) банку(ів) цієї платіжної системи запобігати, протистояти, стримувати та оперативно відновлюватися після кіберінцидентів та кібератак на неї;
27. **Комерційна таємниця (КТ) –** інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.
28. **Контроль доступу** – заходи, які гарантують, що доступ до ресурсів є авторизованим та обмеженим згідно вимог бізнесу та безпеки.
29. **Конфіденційна інформація (КІ) –** інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. До конфіденційної інформації не відносяться таємна та службова інформація.
30. **Конфіденційність** – властивість інформації, яка полягає в тому, що інформація не може бути отримана несанкціонованою особою, об'єктом або процесом.
31. **Надійність** – властивість постійно передбаченої поведінки та результатів.
32. **Неспростовність** – спроможність надати докази появи заявленої події або дії та їх джерела.
33. **Несанкціонований доступ (НСД) –** отримання доступу до комп'ютерної системи або вчинення дій, які призводять до одержання доступу до інформації особою, яка не має прав на перегляд та/або модифікацію цієї інформації без дозволу керівництва або уповноважених ним осіб.
34. **Персональні дані (ПД)** – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.
35. **Платіжна картка (ПК)** – спеціальний платіжний засіб у вигляді емітованої в установленому законодавством порядку пластикової чи іншого виду картки, що використовується для здійснення платіжних операцій з рахунку платника або Товариства, а також інших операцій, установлених відповідним договором.
36. **Подія інформаційної безпеки** – ідентифікований стан системи, служби чи мережі, який вказує на можливе порушення політики інформаційної безпеки чи відмови засобів безпеки, або раніше невідому ситуацію яка може мати відношення до безпеки.
37. **Працівник Товариства** – особа, яка згідно Кодексу законів про працю України має чинні трудові відносини з Товариством.
38. **Процес –** набір упорядкованих дій по створенню та реалізації основних фінансових та інших послуг/продуктів, а також внутрішніх процедур Товариства, що здійснюються за певною технологією і спрямованих на отримання конкретного результату. Процес перетворює вхідні дані на вихідні.
39. **Ресурс** – все, що має цінність та використовується у процесі Товариства.
    До ресурсів, зокрема, відносяться: майно (інформаційні системи та обладнання), інформація, грошові кошти, об'єкти інтелектуальної власності, персонал тощо.

40. **Система управління інформаційною безпекою (СУІБ)** – сукупність політик, процедур, настанов, пов'язаних ресурсів, процесів і дій, якими колективно управляє організація, для захисту своїх інформаційних ресурсів. СУІБ - це системний підхід для розроблення, впровадження, функціювання, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки в організації для досягнення бізнес-цілей.
41. **Товариство** – Товариство з обмеженою відповідальністю «НоваПей».
42. **Управління інцидентами інформаційної безпеки** – процеси для виявлення, реєстрації, оцінювання, реагування, оброблення й дослідження інцидентів інформаційної безпеки.
43. **Цілісність** – властивість точності та повноти.

Терміни, визначення та скорочення, що не визначені у цьому Додатку вживаються у значеннях, наведених далі по тексту Політики, а у разі відсутності такого визначення — у відповідності до законодавства та/або внутрішніх нормативних документів Товариства. Якщо визначення у внутрішніх документах Товариства відрізняються від наведених у цій Політиці, для цілей тлумачення Політики, превалюють значення, наведені у тексті цієї Політики.