ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО
«Нижньодністровська ГЕС»

Додаток 1
до наказу ПрАТ «Нижньодністровська ГЕС»
від « 12 » грудня 2019 р. № 165

П О Л О Ж Е Н Н Я
про порядок реагування та управління інцидентами інформаційної безпеки у ПрАТ «Нижньодністровська ГЕС»

м. Новодністровськ
2019 рік

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1. Це Положення визначає мету, етапи, завдання та основні організаційні заходи щодо порядку реагування та управління інцидентами інформаційної безпеки в інформаційних ресурсах ПрАТ «Нижньодністровська ГЕС» (далі - Товариство). Положення розроблене з урахуванням вимог діючого законодавства України та норм міжнародних стандартів ISO/IEC 18044-2007, ISO/IEC 27000-2012, ISO/IEC 27001-2013, ISO/IEC 27005-2011, ISO/IEC 27035-2015.

2. Вимоги цього Положення є обов'язковими до виконання для всіх працівників Товариства які є користувачами інформаційних ресурсів (бази даних, програмне забезпечення, ресурси локальної мережі, мережі Internet тощо) або мають до них доступ.

3. Всі користувачі повинні ознайомитись з цим Положенням під особистий підпис (Додаток 1 «Лист ознайомлення») та несуть персональну відповідальність за порушення правил цього Положення.

4. Заповнені листи ознайомлення, керівники структурних підрозділів надають: в апараті управління Товариства - до групи АСУ (далі - підрозділ із захисту інформації), - відповідальному за технічний захист інформації (далі - ТЗІ).

5. Пропозиції щодо оновлення вимог цього Положення повинні вноситись за необхідністю. Внесення змін до Положення може проводитись у випадку придбання нових засобів захисту інформації або технічних засобів, що мають функцію захисту інформації і які істотно змінюють встановлений порядок роботи з ними в інформаційних системах Товариства.

6. Відповідальність за внесення змін до Положення несе: в апараті управління Товариства група АСУ - відповідальний за ТЗІ.

7. Організація роботи з виконання вимог цього Положення покладається: в апараті управління Товариства - на групу АСУ.

8. Контроль за виконанням вимог цього Положення забезпечується: в апараті управління Товариства - відповідальними за ТЗІ.

9. Загальна координація заходів з організації роботи та контролю щодо належного виконання вимог цього Положення у Товаристві, здійснюється головним інженером.

10. Працівники групи АСУ (відповідальні за ТЗІ) діють та несуть відповідальність в межах своїх посадових інструкцій та положень про структурні підрозділи.

11. За належне виконання вимог цього Положення, несе відповідальність безпосередньо сам користувач.

2. ТЕРМІНИ ТА ВИЗНАЧЕНЯ

У цьому Положенні наведені терміни вживаються в такому значенні:

- ***актив*** - що-небудь, що має цінність для організації;
  Примітка: Існують різні типи активів: інформація, програмне забезпечення, матеріальні активи (наприклад комп'ютер), послуги, люди і їх кваліфікація, навички та досвід, нематеріальні активи, такі як репутація та імідж.
- ***інформаційний актив (information asset)*** - знання або дані, які мають значення для організації;
- ***атака*** - спроба реалізації загрози;
- ***достовірність (reliability)*** - властивість відповідності передбаченому поведінки і результатами;
- ***доступність*** - властивість інформації бути захищеною від несанкціонованого блокування;
- ***загроза*** - будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС;
- ***інформаційна безпека (information security)*** - збереження конфіденційності, цілісності і доступності інформації;
  Примітка: також сюди можуть бути включені інші властивості, такі як справжність, підзвітність, неспростовності і достовірність.
- ***інцидент інформаційної безпеки (information security incident)*** - одна або декілька небажаних, або несподіваних подій інформаційної безпеки, які зі значним ступенем вірогідності призводять до компрометації операцій бізнесу і створюють загрози для інформаційної безпеки.
- ***конфіденційність*** - властивість інформації бути захищеною від несанкціонованого ознайомлення;
- ***менеджмент ризику (risk management)*** - скоординовані дії по керівництву і управлінню організацією стосовно ризику;
  Примітка: менеджмент ризику зазвичай включає в себе оцінку ризику, обробку ризику, прийняття ризику, комунікацію ризику, моніторинг ризику і перегляд ризику.
- ***неспростовності (non-repudiation)*** - здатність засвідчувати подію або дію, які мали місце і їх суб'єкти таким чином, щоб ці подія або дія і суб'єкти, які мають до цього відношення, не могли бути поставлені під сумнів;
- ***підзвітність (accountability)*** - відповідальність суб'єкта за його дії і рішення;
- ***подія (EFENT)*** - виникнення специфічного набору обставин;
- ***подія в системі інформаційної безпеки (information security EFENT)*** - виявлений стан системи, послуги або стан мережі, що вказує на можливе порушення політики забезпечення інформаційної безпеки, порушення або відмову заходів і засобів контролю та управління або ще невідома ситуація, яка може мати значення для безпеки;
- ***ризик (risk)*** - поєднання ймовірності події і його наслідків;

- ***справжність (authenticity)*** – властивість, що гарантує, що суб'єкт або ресурс ідентичний заявленому;
- ***цілісність*** – властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення.

3. ТИПИ ТА КЛАСИФІКАЦІЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Подією інформаційної безпеки (далі – ІБ) є ідентифікований випадок стану системи, послуги або мережі, що вказує на можливе порушення політики забезпечення інформаційної безпеки, порушення або відмову заходів і засобів контролю та управління або ще невідома ситуація, яка може мати значення для безпеки.

Інцидентом ІБ є одна або декілька небажаних, або несподіваних подій ІБ, які зі значним ступенем вірогідності призводять до компрометації операцій бізнесу і створюють загрози для інформаційної безпеки.

Виникнення події ІБ, не обов'язково означає, що спроба була успішною або що є будь-які наслідки для конфіденційності, цілісності та / або доступності, тобто не всі події ІБ класифікуються як інциденти ІБ.

Загроза може бути реалізована при використанні вразливостей інформаційних ресурсів, послуг або мереж небажаним способом, це є потенційною причиною виникнення подій ІБ та інцидентів з інформаційними активами, які мають вразливості.

Відношення між об'єктами в ланцюгу інциденту ІБ показано на рисунку 1.

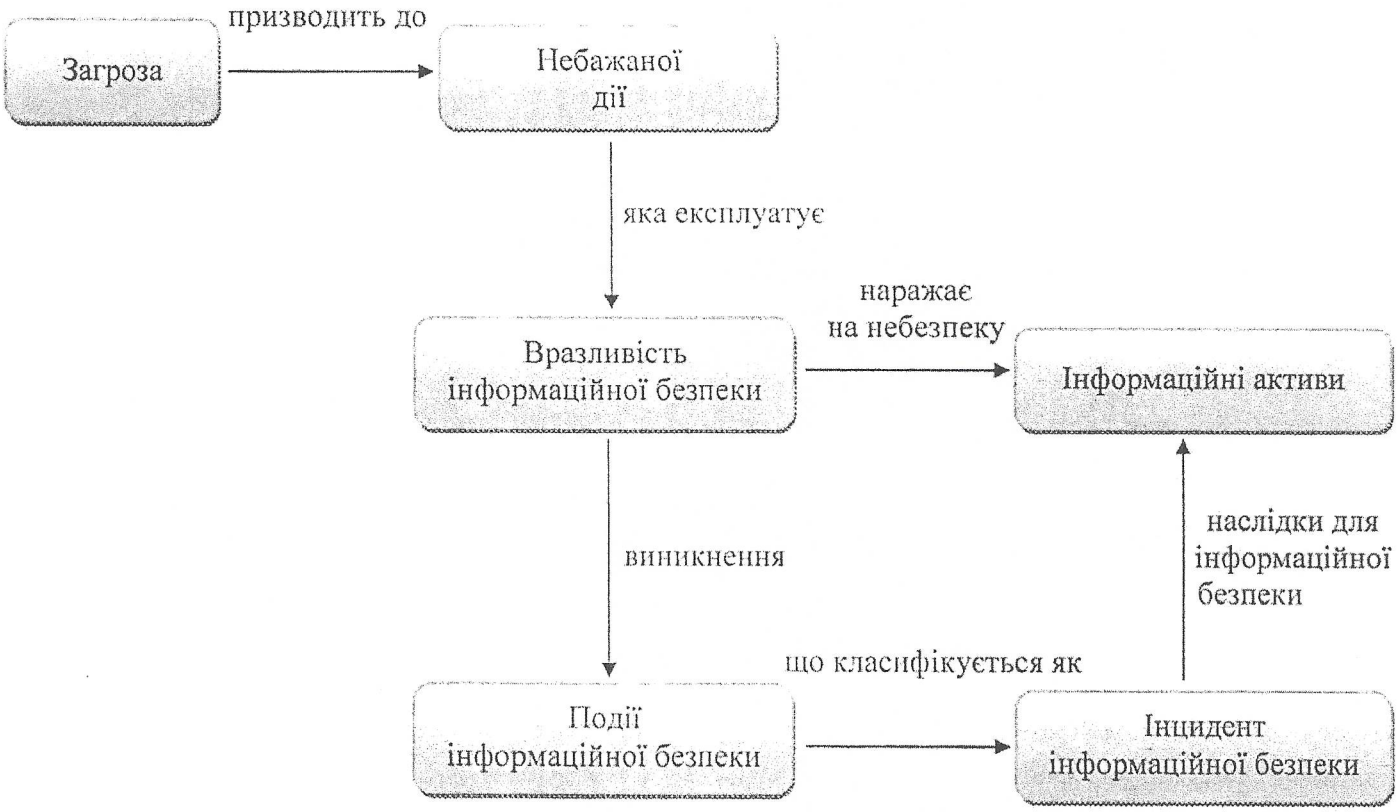

Рисунок 1 – Об'єкти ланцюга інциденту ІБ

Інциденти ІБ можуть бути навмисними або випадковими і можуть бути викликані як технічними, так і не технічними засобами.

В даний час спостерігається значне зростання числа інцидентів ІБ які фіксуються в організаціях, що мають як внутрішній, так і зовнішній характер.

За типом виникнення, інциденти ІБ поділяються на внутрішні і зовнішні.

Внутрішній інцидент - це інцидент, джерелом якого є порушник, пов'язаний з постраждалою стороною безпосереднім чином (трудовим договором або іншим способом). Серед системних подій такого типу можна виділити наступні найбільш поширені:

- витік інформації з обмеженим доступом;
- несанкціонований доступ до інформації;
- видалення інформації;
- компрометація інформації;
- саботаж;
- шахрайство за допомогою ІТ;
- аномальна мережева активність;
- аномальна поведінка бізнес-додатків та іншого ПЗ;
- використання активів компанії в особистих цілях або в шахрайських операціях.

Зовнішній інцидент - це інцидент, джерелом якого є порушник, що не пов'язаний з постраждалою стороною безпосереднім чином, серед системних подій такого типу можна виділити наступні найбільш поширені:

- шахрайство в інформаційних ресурсах;
- атаки типу «відмова в обслуговуванні» (DoS), в тому числі розподілені (DDoS);
- перехоплення і підміна трафіка;
- неправомірне використання корпоративного бренду в мережі Інтернет;
- фішинг, вішинг;
- розміщення конфіденційної / провокаційної інформації в мережі Інтернет;
- злом, спроба злому, сканування порталу компанії;
- сканування мережі, спроба злому мережевих вузлів;
- вірусні атаки;
- несанкціонований доступ до інформації з обмеженим доступом;
- анонімні листи (листи з погрозами, пропозиціями тощо).

Інциденти ІБ класифікуються за наступними ознаками:

- за ступенем тяжкості наслідків для діяльності Товариства (в грошовому вираженні, за бальною шкалою);
- за ступенем ймовірності повторного виникнення інциденту ІБ;
- за видами джерел загроз ІБ, що викликають інциденти ІБ;
- за навмисністю виникнення інциденту ІБ (випадковий, навмисний, помилковий);
- за видами об'єктів інформаційної інфраструктури, задіяних (уражених) при

реалізації інциденту ІБ;

- за рівнем інформаційної інфраструктури, на якому відбувається інцидент ІБ;
- по порушеним властивостям інформаційної безпеки (конфіденційність, цілісність, доступність);
- за типом інциденту ІБ (здійснений інцидент ІБ, спроба здійснення інциденту ІБ);
- по області поширення і дії інциденту ІБ (в межах Товариства, в межах апарату управління (Товариства), в межах одного структурного підрозділу, в межах одного користувача;
- за складністю виявлення інциденту ІБ;
- за складністю закриття інциденту ІБ.

Приклади інцидентів

Можливі порушення вимог конфіденційності:

- Інциденти, через які отримано несанкціонований доступ до інформації;
- Втрата носіїв інформації за межами приміщення;
- Втрата або крадіжка ноутбука;
- Спроби персоналу організації отримати доступ вище наявного рівня;
- Спроби зсередини або ззовні отримати доступ до систем (злам).

Можливі порушення вимог цілісності:

- Втрата даних або незавершені транзакції;
- Віруси, «троянські коні» (шкідливе програмне забезпечення);
- Пошкоджені сектора на жорстких дисках, помилки парності і пам'яті;
- Невірні контрольні суми або значення хеш-функцій.

Можливі порушення вимог доступності:

- Простої в роботі протягом неприйнятного періоду часу. Якщо простій триває довше, ніж обумовлено в Угоді про Рівні Послуг і не може бути усунутий протягом певного часу, вступає в силу надзвичайний план;
- Віруси, «троянські коні»;
- Крадіжка ноутбуків, комплектуючих або носіїв інформації.

4. РЕАГУВАННЯ ТА УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1. Загальні відомості

Ознайомлення користувачів інформаційних ресурсів Товариства з порядком реагування та управління інцидентами ІБ забезпечується ознайомленням під розпис з цим Положенням після його затвердження, а також після його перегляду (за необхідністю).

Реагування на інцидент ІБ включає в себе технічні заходи, що забезпечують цілісність криміналістично важливих даних та можливість судового дослідження цих даних в майбутньому, а також організаційні заходи, які дозволяють знизити збиток від інциденту і скласти документи необхідні для правоохоронних органів.

Технічні заходи полягають в негайному забезпеченні цілісності даних, які потенційно мають відношення до інциденту ІБ, шляхом відключення, упаковки, опечатування і належного зберігання відповідних носіїв інформації. Відключення носіїв інформації дозволяє звести до нуля ризик знищення криміналістично важливих даних в результаті роботи шкідливих програм і дій зловмисника, а їх упаковка, опечатування та належне зберігання забезпечують достатній рівень достовірності результатів криміналістичного дослідження в суді.

Організаційні заходи полягають в повідомленні керівництва організації, підрозділів (служб) інформаційної безпеки (захисту інформації) організації та інших зацікавлених організацій про факт інциденту ІБ. Документи, складені при проведенні організаційних заходів, можуть використовуватися як підстави для розгляду питань про порушення кримінальних справ або для уточнення питань, які виносяться на розгляд при призначенні криміналістичних (судових) та інших експертиз носіїв інформації організації.

Після реагування на інцидент ІБ починається розслідування інциденту і відновлення інформаційної системи організації. Відновлення інформаційної системи організації полягає в заміні вилучених, упакованих та опечатаних носіїв інформації на нові, встановлення необхідного ПО і конфігурації інформаційної системи з урахуванням підвищених вимог політики ІБ.

Організація процесу реагування на інцидент переслідує такі цілі:

- попередити нескоординовані дії і в найкоротші терміни відновити працездатність інформаційних ресурсів при виникненні інциденту ІБ;
- надати деталізований звіт про інцидент ІБ і рекомендації щодо цього інциденту;
- створити умови для накопичення і зберігання точної інформації про інциденти ІБ;
- забезпечити швидке виявлення та / або попередження подібних інцидентів ІБ в майбутньому (шляхом аналізу інцидентів, які трапилися в минулому, зміни політики ІБ, модернізації системи ІБ);
- забезпечити збереження і цілісність доказів інциденту;
- створити умови для порушення цивільної або кримінальної справи проти зловмисника;
- мінімізувати порушення порядку роботи і пошкодження даних ІТ-системи;
- мінімізувати наслідки порушення конфіденційності, цілісності та доступності ІТ-системи;
- захистити репутацію Товариства і його інформаційні ресурси;
- провести навчання співробітників реагування на інцидент.

У загальному випадку алгоритм реагування на інциденти ІБ, представлений на рисунку 2.

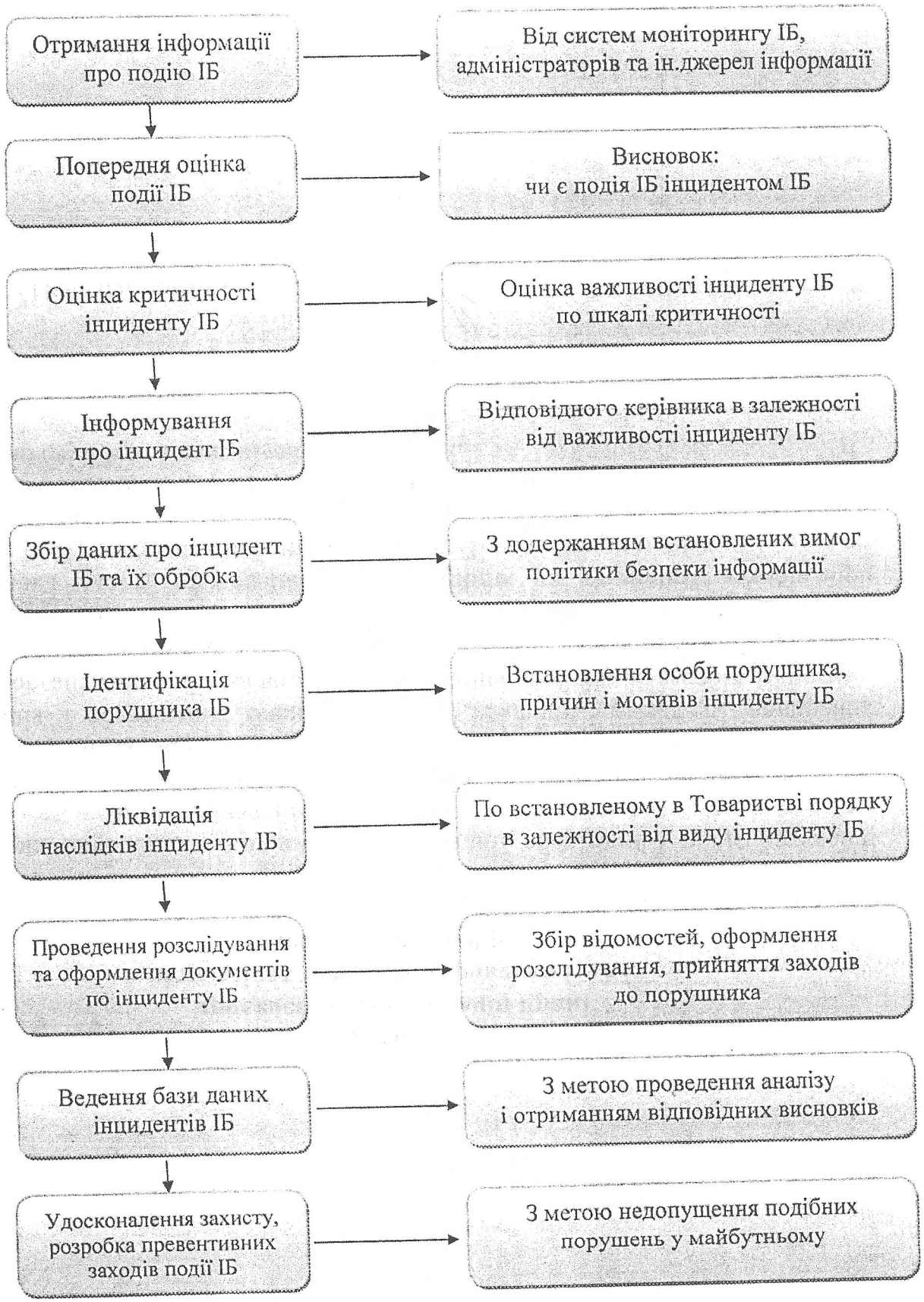

Рисунок 2 – Загальний алгоритм реагування на інциденти ІБ

4.2. Виявлення інцидентів інформаційної безпеки

Основними джерелами інформації про інциденти ІБ є:

- факти, виявлені керівником структурного підрозділу, працівниками підрозділу із захисту інформації (відповідальними за ТЗІ), працівниками структурного підрозділу з інформаційних технологій, а також іншими працівниками Товариства.
- результати роботи засобів моніторингу ІБ, результати перевірок та аудиту (внутрішнього або зовнішнього);
- журнали та оповіщення операційних систем серверів і робочих станцій, антивірусної системи, системи резервного копіювання та інших систем;
- звернення суб'єктів персональних даних із зазначенням інциденту ІБ;
- запити і розпорядження органів нагляду за дотриманням прав суб'єктів персональних даних;
- інші джерела інформації.

Користувач інформаційних ресурсів Товариства може виявити ознаки наявності інциденту ІБ шляхом аналізу поточної ситуації на предмет її відповідності вимогам політики безпеки інформації, що впроваджені в Товаристві.

Події ІБ можуть бути виявлені будь-яким користувачем інформаційних ресурсів Товариства. Крім того, події ІБ можуть виявлятися автоматично: пристроями аналізу записів аудиту, міжмережевими екранами, системами виявлення вторгнень, антивірусними програмами тощо.

Користувач інформаційних ресурсів Товариства, виявивши подію, що потрапляє під категорію подій ІБ цього Положення, повинен негайно довести цю інформацію до відома працівників підрозділу із захисту інформації (відповідальними за ТЗІ) та працівників структурного підрозділу з інформаційних технологій по телефону або за допомогою електронної пошти, докладно описавши подію у довільній формі.

4.3. Аналіз вихідних даних і прийняття рішення про проведення розгляду інцидентів інформаційної безпеки

Працівник групи АСУ (відповідальний за ТЗІ), після отримання інформації про можливий інцидент ІБ негайно проводить первинний аналіз отриманих даних. У процесі аналізу перевіряється наявність виявленого факту порушення.

На розсуд працівника, який проводить перевірку, одиничний інцидент ІБ, що не призвів до негативних наслідків і був здійснений користувачем Товариства вперше, фіксується працівниками групи АСУ (відповідальними за ТЗІ) в картці даних «Інциденти ІБ» (Додаток 2) з присвоєнням статусу «Розгляд не потрібен».

У разі наявності ознак інциденту ІБ, що призвів до негативних наслідків, працівник групи АСУ (відповідальний за ТЗІ) класифікує інцидент, визначає попередню ступінь критичності інциденту ІБ і приймає рішення про необхідність проведення розгляду, інформує керівника свого структурного підрозділу про інцидент ІБ, ініціює формування реєстраційної картки інциденту з присвоєнням йому статусу «В процесі розгляду».

В термін не більше 3 (трьох) робочих днів з моменту надходження інформації про інциденті ІБ, працівник групи АСУ (відповідальний за ТЗІ) за погодженням з керівником

структурного підрозділу в якому було виявлено інцидент ІБ, визначає і ініціює першочергові заходи, спрямовані на локалізацію інциденту ІБ і на мінімізацію його наслідків.

4.4. Розгляд інциденту інформаційної безпеки

Відповідальний за ТЗІ оперативно аналізує зареєстровану подію ІБ, після чого має право отримати будь-які уточнення у користувача, який надіслав повідомлення про подію ІБ, а також зібрати і зберегти необхідну додаткову інформацію, яка є доступною. В ході збору додаткової інформації може також задокументувати такі відомості:

- проведені заходи, включаючи використані кошти;
- спосіб верифікації свідоцтва (якщо є);
- місця зберігання свідоцтва наявності події ІБ;
- деталі зберігання матеріалів і подальшого доступу до них.

Інформація та інші свідчення, зібрані і збережені на цьому етапі, можуть знадобитися в майбутньому для дисциплінарного або судового розгляду.

Мета розгляду інцидентів ІБ це:

- розробка організаційних і технічних рішень, спрямованих на зниження ризиків порушення ІБ, запобігання і мінімізацію подібних порушень в майбутньому;
- захист прав користувачів, встановлених діючим законодавством України;
- захист репутації Товариства і його інформаційних ресурсів;
- забезпечення безпеки персональних даних;
- запобігання несанкціонованому доступу до інформації з обмеженим доступом (таємної, службової, конфіденційної), яка підлягає захисту згідно діючого законодавства України і (або) запобігання передачі їх особам, які не мають права доступу до такої інформації.

Розгляд інциденту ІБ складається з наступних етапів:

- підтвердження / спростування факту виникнення інциденту ІБ;
- класифікація інциденту ІБ за встановленими критеріями (розділ 3);
- підтвердження / коригування рівня критичності інциденту ІБ;
- уточнення додаткових обставин (деталей) інциденту ІБ;
- отримання (збір) доказів виникнення інциденту ІБ, забезпечення їх збереження і цілісності;
- мінімізація наслідків інциденту ІБ;
- інформування та консультування персоналу Товариства по діям виявлення, усунення наслідків і запобігання інцидентів ІБ;
- переоцінка ризиків, що призвели до виникнення інциденту, актуалізація необхідних положень, регламентів, правил ІБ.

Порядок проведення розгляду інциденту ІБ:

В процесі проведення розгляду інциденту ІБ обов'язковими для встановлення є:

- дата і час здійснення інциденту ІБ;
- ПІБ, посада і підрозділ порушника ІБ;

- класифікація інциденту;
- рівень критичності інциденту ІБ;
- обставини і мотиви скоєння інциденту ІБ;
- інформаційні ресурси, порушені інцидентом ІБ;
- характер і розмір реального і потенційного збитку;
- обставини, що сприяли вчиненню інциденту ІБ.

4.5. Реагування на інцидент ІБ

Після підтвердження інциденту ІБ, працівник групи АСУ (відповідальний за ТЗІ) забезпечує виконання дій щодо негайного реагування на інцидент ІБ, реєстрації подробиць в БД інцидентів ІБ і повідомленню користувачів про необхідні дії щодо інциденту ІБ.

Якщо критичність інциденту ІБ визнається високою, відповідальний за ТЗІ негайно повідомляє про інцидент ІБ свого безпосереднього керівника з метою доведення факту інциденту ІБ до відома Генерального директора Товариства.

При виконанні дій щодо негайного реагування відповідальному за ТЗІ необхідно враховувати наступні фактори:

- при прийнятті відповідного рішення необхідно оцінити технічну можливість швидко та надійно відключити інформаційний ресурс, який був атакований (комп'ютер, базу даних, ПЗ, сервіс, мережу тощо);
- запобігання повторного появи інциденту ІБ є пріоритетним завданням, оскільки порушник виявив слабке місце, яке необхідно оперативно усунути;
- необхідність дбати про безпеку і належне оформлення доказів;
- при проведенні дослідження джерел інформації потрібно забезпечити незмінність доказів, слід працювати тільки з їх копіями і зберігати всю зібрану інформацію на носіях, доступних тільки для читання.

При інциденті ІБ, що не поширюється за межі більше ніж одного структурного підрозділу, відповідальний за ТЗІ інформує про факт інциденту ІБ керівника відповідного структурного підрозділу.

При інциденті ІБ, що поширюється за межі більше, ніж одного структурного підрозділу (відділу), відповідальний за ТЗІ інформує про факт інциденту ІБ керівника відповідного структурного підрозділу та ініціює проведення розгляду інциденту ІБ.

З метою мінімізації наслідків інциденту ІБ на час проведення розслідування начальник відповідного підрозділу за вказівкою відповідального за ТЗІ повинен негайного відключити вірогідного порушника ІБ (без погодження з керівником його структурного підрозділу) від інформаційних ресурсів Товариства та / або блокування облікового запису (прав доступу) порушника ІБ. Інформація про відключення (припинення прав доступу), направляється відповідальним за ТЗІ керівнику структурного підрозділу вірогідного порушника ІБ.

Працівник підрозділу із захисту інформації (відповідальний за ТЗІ) в процесі розгляду і проведення розслідування інциденту ІБ при необхідності, має право запрошувати інформацію в будь-яких структурних підрозділах. Запит направляється на ім'я керівника структурного підрозділу з обов'язковим зазначенням термінів надання інформації (з урахуванням необхідності її аналізу, збору і підготовки).

Після отримання необхідної інформації по інциденту ІБ, працівник групи АСУ (відповідальний за ТЗІ) здійснює розгляд і проводить аналіз отриманих даних.

Керівник структурного підрозділу, в якому трапився інцидент, протягом 3 (трьох) робочих днів з моменту виявлення інциденту ІБ зобов'язаний надати відповідальному за ТЗІ службову записку від порушника ІБ. Службова записка повинна бути складена на ім'я директора департаменту фізичного захисту, режиму та безпеки і підписана порушником ІБ і безпосереднім керівником його структурного підрозділу.

У разі, якщо порушник ІБ або керівник його структурного підрозділу відмовились надати або не надали у визначений термін службову записку стосовно виявленого інциденту ІБ, працівник підрозділу із захисту інформації (відповідальний за ТЗІ) складає про це акт у довільній формі на ім'я Генерального директора Товариства.

Коли інцидент ІБ опрацьований, то оновлюється запис про інцидент в БД (журналі) інцидентів ІБ.

Всю інформацію про опрацьований інцидент ІБ відповідальний за ТЗІ надає своєму безпосередньому керівнику для прийняття подальшого рішення відповідно до отриманих результатів щодо інциденту ІБ.

4.6. Оцінка інциденту ІБ і заподіяної ним шкоди

Підтвердження і оцінка інциденту ІБ входять в обов'язки групи АСУ (відповідального за ТЗІ) і мають бути виконані в найкоротший термін.

Якщо за результатами розгляду наявної інформації подія ІБ визначається як помилкова тривога, то про це відповідальний за ТЗІ інформує користувача, який повідомив про подію ІБ, по електронній пошті.

Якщо виявлена подія ІБ розглядається працівником групи АСУ (відповідальним за ТЗІ) як інцидент ІБ, то в максимально стислі терміни здійснюється подальша оцінка інциденту ІБ:

- інцидент ІБ ПС класифікується за встановленими критеріями (розділ 3);
- атрибути класифікації заносяться в БД інцидентів.

Працівник групи АСУ (відповідальний за ТЗІ) проводить оцінку негативних наслідків від реалізації інциденту ІБ. В ході даної оцінки враховуються:

- прямий фінансовий збиток;
- репутаційний збиток;
- потенційний збиток;
- непрямі втрати, що пов'язані з недоступністю сервісів, втратою інформації;
- інші види шкоди або аспекти негативних наслідків для Товариства або суб'єктів персональних даних.

У разі, якщо на час проведення розгляду інциденту ІБ порушник ІБ був відключений від інформаційних ресурсів Товариства (заблокований його обліковий запис), то за результатами розгляду інциденту ІБ відповідальний за ТЗІ дає вказівку начальнику відповідного підрозділу Товариства щодо відновлення в повному або обмеженому обсязі раніше наявних у порушника ІБ прав доступу до інформаційних ресурсів Товариства або ініціює офіційну процедуру скасування (зміни) прав доступу.

Якщо порушення ІБ було викликано незнанням порушником ІБ правил (технології) роботи з інформаційними ресурсами, то підставою для повернення прав доступу є успішне проходження інструктажу із захисту інформації, ознайомленням з положеннями посадової інструкції та іншими розпорядчими документами Товариства.

Відновлення тимчасово відключених у порушника ІБ прав доступу до інформаційних ресурсів Товариства (розблокування облікового запису) може проводитися за розпорядженням начальника відповідного підрозділу Товариства тільки за вказівкою відповідального за ТЗІ.

4.7. Офомлення результатів проведеного розгляду інциденту

Інформація, зібрана в процесі розгляду інцинденту ІБ, фіксується у відповідального за ТЗІ в картотеці даних «Інциденти ІБ» і враховується при підготовці підсумкового висновку по інциденту ІБ (додаток 2).

Відповідальний за ТЗІ формує, погоджує з усіма учасниками розгляду і підписує підсумковий висновок з розслідування інциденту ІБ.

Підсумковий висновок по інциденту ІБ відповідальний за ТЗІ направляє керевникам структурних підрозділів, пов'язаних з інцидентом ІБ.

Відповідальний за ТЗІ фіксує завершення розгляду в картці «Інциденти ІБ» і надає інциденту ІБ статус «Закритий».

При необхідності визначення правової оцінки інциденту ІБ відповідальний за ТЗІ, передає всю необхідну інформацію до юридичного підрозділу.

У разі виявлення в інциденті ІБ ознак адміністративного правопорушення чи кримінального злочину, що належать до сфери інформаційних технологій, керівник юридичного підрозділу передає всі матеріали по інциденту ІБ керівнику Товариства для прийняття рішення про подачу заяви до правоохоронних органів України.

4.8. Закінчення розгляду інциденту інформаційної безпеки, превентивні заходи

Після прийняття рішення про закриття інциденту ІБ має бути проведена (у разі необхідності) подальша технічна експертиза і аналіз з метою визначення засвоєних уроків і потенційних поліпшень ІБ і системи управління інцидентами ІБ.

<u>подальша технічна експертиза</u>

У разі необхідності проведення додаткової технічної експертизи інциденту ІБ після його закриття, відповідальний за ТЗІ організовує її проведення відповідно до п. 4.5. цього Положення. Перелік питань при проведені експертизи щодо порушень (злочинів) в сфері інформаційної безпеки (кібербезпеки) (Додаток 3).

<u>висновки з інциденту ІБ</u>

Після завершення інциденту ІБ, важливо швидко опрацювати висновки, які були зроблені в процесі з розгляду цього інциденту і вжити відповідних заходів щодо:

- нових або змінених вимог до заходів захисту для забезпечення ІБ;
- змін в системі управління інцидентами ІБ і її процедурах, формах звіту і баз даних інцидентів ІБ.

<u>визначення покращень безпеки</u>

У процесі аналізу, проведеного після розгляду інциденту ІБ, можуть бути визначені нові необхідні захисні заходи. Розроблені рекомендації та відповідні їм вимоги до заходів захисту реалізуються на основі Плану впровадження заходів інформаційної безпеки.

Якщо інцидент ІБ мав високу критичність, відповідальний за ТЗІ після його розгляду доповідає своєму безпосередньому керівнику про необхідність проведення наради всіх зацікавлених осіб, що володіють інформацією про інцидент. На нараді розглядаються наступні питання:

- чи працювали належним чином процедури, прийняті в цьому Положенні;
- чи існують інші процедури або методи, які сприяли б виявленню інцидентів ІБ;
- чи були визначені процедури або засоби, які використовувалися б в процесі реагування;
- чи застосовувалися процедури, що допомагають відновленню інформаційних ресурсів після ідентифікації інциденту ІБ;
- чи була передача інформації про інцидент ІБ від всіх причетних сторін ефективною в процесі виявлення, інформування та реагування.

Результати наради документуються і враховуються при підготовці Плану впровадження заходів інформаційної безпеки.

Крім того, по завершенню розгляду інциденту ІБ, відповідальний за ТЗІ передає наявні матеріали (в обсязі, достатньому для прийняття рішення) вищестоящому керівнику порушника ІБ для вирішення питання про притягнення порушника ІБ до дисциплінарної відповідальності.

На підставі отриманих результатів розгляду керівник структурного підрозділу в якому був виявлений інцидент ІБ спільно з відповідальний за ТЗІ в термін не більше 3 (трьох) робочих днів, організовує проведення одного або декількох заходів, спрямованих на зниження ризиків інформаційної безпеки в майбутньому:

- аналіз і перегляд наявних прав доступу до інформаційних ресурсів у порушника ІБ;
- доведення до відома всіх співробітників структурного підрозділу вимог внутрішніх нормативних документів Товариства із захисту інформації;
- обговорення інциденту ІБ на нараді керівників, тренінгах або зборах колективу;
- скасування у порушника неактуальних прав доступу до інформаційних ресурсів;
- проведення заходів, спрямованих на запобігання несанкціонованого доступу до конфіденційної інформації, інформації, що містить комерційну таємницю, персональних даних і (або) передачі їх особам, які не мають права доступу до такої інформації;

За необхідністю, відповідальний за ТЗІ доводить результати проведеного розгляду інциденту ІБ до відома керівника Товариства.

4.9. Реалізація покращень системи управління інцидентами ІБ

У процесі аналізу, проведеного після розгляду інциденту ІБ, можуть бути визначені нові необхідні захисні заходи. Розроблені рекомендації та відповідні їм вимоги до заходів захисту реалізуються на основі Плану впровадження заходів інформаційної безпеки.

Етап покращення системи управління інцидентами ІБ ґрунтується на рекомендаціях, сформованих в ході етапу аналізу інцидентів ІБ (п.4.8. цього Положення).

Залежно від серйозності (критичності) інциденту ІБ і ступеня його впливу при оцінці результатів аналізу ризиків ІБ і системи управління інцидентами ІБ, є вірогідність врахування нових загроз і вразливостей. В результаті завершення аналізу ризиків ІБ і системи управління інцидентами ІБ може знадобитись внесення змін в існуючі або впровадження нових заходів захисту.

Згідно рекомендацій, зроблених в процесі аналізу інциденту ІБ, відповідальний за ТЗІ ініціює і організовує процес впровадження оновлених і (або) нових заходів захисту відповідно до Плану впровадження заходів інформаційної безпеки, затвердженого Генеральним директором Товариства.

4.10. Права та обов'язки учасників розгляду інциденту інформаційної безпеки

Відповідальний за ТЗІ має право:

- вимагати від безпосереднього керівника порушника ІБ надання письмових пояснень щодо обставин скоєння інциденту ІБ;
- здійснювати взаємодію з керівниками і співробітниками Товариства в рамках їх компетенцій, отримувати усні і письмові роз'яснення та іншу інформацію, необхідну для проведення розгляду інциденту ІБ;
- ініціювати відключення від інформаційних ресурсів користувачів, які порушили правила або вимоги ІБ, на період проведення розслідування інциденту ІБ в разі, якщо є істотний ризик того, що продовження роботи співробітника з ІР може спричинити значне збільшення збитку або нові інциденти ІБ;
- за результатами розслідування інциденту ІБ ініціювати зміни в бізнес-процесах і інформаційних ресурсах Товариства з метою підвищення їх захищеності і зниження ризиків інцидентів ІБ;
- ініціювати процедури притягнення порушника ІБ до дисциплінарної та (або) матеріальної відповідальності згідно з внутрішніми нормативними документами Товариства.

Відповідальний за ТЗІ зобов'язаний:

- об'єктивно проводити розгляд кожного інциденту ІБ;
- визначати першочергові заходи, спрямовані на локалізацію інциденту ІБ і мінімізацію негативних наслідків;
- фіксувати в картці даних «Інциденти ІБ» всю вихідну інформацію про Інциденти ІБ і результати її розслідування;
- надавати звіти і рекомендації по проведеним розглядів керівництву Товариства;
- проводити аналіз обставин, що сприяли вчиненню кожного інциденту ІБ, і на його основі, спільно з відділом інформаційних технологій, розробляти рекомендації і пропозиції щодо оптимізації бізнес-процесів і зниження шкоди від подібних інцидентів ІБ і мінімізації можливості їх повторення в майбутньому.

Керівники та працівники структурних підрозділів зобов'язані:

- надавати за запитами групи АСУ (відповідального за ТЗІ) усні та письмові роз'яснення та іншу інформацію в межах своєї компетенції, необхідну для проведення розгляду інциденту ІБ;
- інформувати групу АСУ (відповідального за ТЗІ) про виявлені інциденти ІБ;
- інформувати відповідального за ТЗІ про наявні запити та звернення суб'єктів персональних даних.

5. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

5.1. До порушника інформаційної безпеки можуть бути застосовані заходи стягнення в порядку встановленому чинним законодавством України.

6. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

6.1. Контроль за виконанням цього Положення у Товаристві покладається на групу АСУ з відповідальним за ТЗІ.

6.2. Зміни до цього Положення вносяться наказами Товариства на підставі змін нормативно-правових актів України та вимог нормативних документів Товариства.

6.3. Дане Положення вступає в силу з моменту його затвердження наказом Товариства.

Відповідальний за ТЗІ  Козак М.В.