

ПЛАН РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Типова процедура

1. Загальні положення.

Інцидент інформаційної безпеки (інцидент ІБ) – це поодинокі подія, або ряд небажаних та непередбачених подій інформаційної безпеки (ІБ), через які існує ймовірність компрометації інформації ЗНУ та загрози інформаційній безпеці. До інцидентів ІБ відносяться:

- технічний збій та відмови в роботі комп'ютерної та обчислювальної техніки, інших ІТ-систем;
- порушення конфіденційності та цілісності інформації;
- недотримання вимог ІБ (порушення політик інформаційної безпеки ЗНУ);
- зовнішні або внутрішні зловмисні дії, пов'язані з незаконним моніторингом інформаційних систем, завантаженням/сприянням у проникненні до комп'ютерної мережі та ІТ-систем ЗНУ шкідливого програмного забезпечення тощо;
- зберігання ключів кваліфікованого електронного підпису (КЕП) на жорстких дисках ПК;
- наявність відкритих мережевих каталогів загального доступу;
- наявність програмного забезпечення, забороненого відповідно до законодавства України (рішення РНБО, Указ Президента України 601/2024 від 02.09.2024);
- порушення положень про порядок надання доступу користувачам до інформаційних систем (наприклад передача іншій особі або розголошення особистого паролю).

Цілями Плану реагування на інциденти ІБ є:

- відновлення штатної роботи комп'ютерної та обчислювальної техніки, інших ІТ-систем у найкоротші терміни;
- зведення до мінімуму впливу інцидентів ІБ на роботу ЗНУ;
- забезпечення виявлення та фіксації всіх інцидентів ІБ;
- залучення всіх необхідних сил та засобів для реагування на інциденти ІБ;
- здійснення необхідних заходів для запобігання або зменшення кількості інцидентів ІБ в подальшому.

Задачами Плану реагування на інциденти ІБ є:

- оперативний моніторинг стану інформаційної безпеки ЗНУ;
- виявлення, облік, реагування, розслідування та аналіз інцидентів ІБ;
- інформування керівництва та зацікавлених сторін про стан ІБ.

2. Управління інцидентами ІБ.

Управління інцидентами ІБ в ЗНУ складається з наступних заходів:

- Виявлення та повідомлення про інцидент ІБ;
- Дії користувача після виявлення інциденту ІБ;
- Реагування на інцидент ІБ;
- Розслідування інциденту ІБ;
- Повідомлення про інцидент ІБ всіх зацікавлених сторін;
- Профілактика інцидентів ІБ.

2.1. Виявлення та повідомлення про інциденти ІБ.

1. Будь-який працівник, якому стало відомо про інцидент ІБ, не пізніше ніж протягом 1 (однієї) години з моменту виявлення повідомляє про це свого безпосереднього керівника, керівника центру інформаційних систем та комп'ютерних технологій та відповідального за ІБ.

2. Повідомлення також повинно бути відправлено в системі HELP на адресу <https://help.znu.edu.ua/> не пізніше ніж протягом 1 (однієї) години після виявлення можливого порушення.

3. Безпосередній керівник та/або відповідальний за ІБ перевіряє обставини можливого порушення та невідкладно вживає можливі заходи реагування на порушення, а також доповідає про порушення керівництву ЗНУ. Інформація про інцидент фіксується відповідальним за ІБ у Журналі подій інформаційної безпеки.

4. Для негайного повідомлення про порушення працівники можуть також відправити повідомлення відповідальному за ІБ за вказаною адресою: security@znu.edu.ua.

2.2. Дії користувача після виявлення інцидента ІБ.

Користувач повинен дотримуватися правильної поведінки у разі події інформаційної безпеки, тобто:

1) не вимикати та не перезавантажувати комп'ютер (для збереження стану оперативної пам'яті та журналів подій);

2) від'єднати мережевий кабель або вимкнути Wi-Fi;

3) не намагатися самостійно видалити або відновлювати файли;

4) негайно записувати усі важливі подробиці (час виникнення, тип невідповідності або порушення, збій, який мав місце, повідомлення на екрані, незвичайний режим роботи);

5) не виконувати жодних власних дій, а негайно звітувати контактній особі;

6) не повідомляти про інцидент третім особам без санкції керівника.

2.3. Реагування на інцидент.

Відповідальний за ІБ при отриманні повідомлення про інцидент ІБ самостійно або із залученням відповідних працівників ЗНУ вживає наступні заходи, з метою обмеження наслідків порушення чи інциденту:

1. Вживає заходів по збиранню та збереженню доказів та припиняє несанкціоновану дію.

2. Відключає або локалізує комп'ютерну та/або ІТ-систему, яка може бути уражена.

3. По можливості відновлює записи, дані, що могли постраждати.

4. По можливості усуває вразливості та слабкі місця, які призвели до інциденту.

5. За рішенням керівника ЗНУ повідомляє правоохоронні органи (CERT-UA, кіберполіцію) про інцидент безпеки та його ознаки.

Вказані пункти виконуються виключно у встановленому порядку. Відновлення записей та даних, що могли постраждати, необхідно починати лише після письмової фіксації стану системи та завершення збору доказів.

2.4. Розслідування та мінімізація ризиків

1. При інциденті ІБ, що може причинити значні негативні наслідки, відповідальний за ІБ долучає до розслідування членів робочої групи з інформаційної безпеки (РГІБ). До РГІБ також долучається керівник відділу/підрозділу, де трапився інцидент.

2. Група розглядає обставини, причини та наслідки інциденту ІБ та оцінює ризики ІБ, які пов'язані з інцидентом. При цьому розглядаються наступні фактори, але не обмежуються ними:

- характер цифрового активу, який постраждав в наслідок інциденту, та його важливість для функціонування ЗНУ;

- необхідні заходи та засоби для відновлення функціонування;

- договірні зобов'язання, які можуть бути не виконані, порушені;
- ризики крадіжки особистих даних або втрати інформації в наслідок її псування, затирання чи шифрування, можливості щодо відновлення якомога актуальнішої версії резервного копіювання;
- ризик заподіяння шкоди репутації ЗНУ;
- обсяги (масив) втраченої, вкраденої чи зіпсованої інформації.

2.5. Аналіз порушення та запобігання повторенню.

1. Після вжиття негайних заходів для зменшення ризиків, пов'язаних з порушенням, відповідальний за ІБ проводить розслідування причин порушення. Строки розслідування наступні: підготовка попереднього звіту - протягом 3 робочих днів; проведення повного розслідування - протягом 10–30 робочих днів залежно від складності інциденту.

При необхідності разом із розслідуванням може проводитися аудит безпеки фізичних, організаційних і технологічних заходів.

2. Для проведення розслідування причин інциденту відповідальний за ІБ залучає відповідних працівників ЗНУ та при необхідності зовнішніх експертів.

3. Результати розслідування доповідаються керівництву ЗНУ (разом з рекомендаціями щодо запобігання подібних інцидентів у майбутньому) не пізніше ніж через 5 робочих днів після завершення розслідування.

4. За результатами складається план заходів з усунення недоліків, виявлених у ході розслідування інциденту, якщо це доречно.

2.6. Профілактика інцидентів ІБ.

Профілактика інцидентів ІБ складається з наступних кроків:

- 1) Щорічні навчання персоналу з питань ІБ.
- 2) Щорічні планові перевірки стану ІБ згідно затвердженого графіка.
- 3) Проведення тестових навчань із реагування на інциденти.

Поінформованість з безпеки, освіта та навчання повинні охоплювати інформацію щодо відомих загроз, належних каналів і процедур звітування щодо інцидентів ІБ і особи, з якою контактувати для отримання подальших рекомендацій із безпеки.

Навчання для поліпшення поінформованості призначені для того, щоб надати можливість працівникам усвідомити проблеми та інциденти ІБ і реагувати згідно з потребами їхніх посадових ролей.

Інциденти ІБ можна використовувати у навчанні користувачів для поінформованості як приклади того, що може трапитись, як реагувати на такі інциденти і як уникнути їх у майбутньому. Щоб бути здатними правильно враховувати події та інциденти ІБ, необхідно збирати докази якнайшвидше після того, як вони відбулися. Збої або інша аномальна поведінка системи можуть бути показником атаки на безпеку або фактичного порушення безпеки і тому про них треба завжди звітувати як про подію ІБ.

План реагування на інциденти ІБ потрібно переглядати не рідше ніж один раз на рік або позапланово після кожного значного інциденту.