БОРИСПІЛЬСЬКИЙ МІСЬКИЙ ГОЛОВА

Р О З П О Р Я Д Ж Е Н Н Я

21 листопада 2025 року № 153

м. Бориспіль Київської області

Про затвердження Політики інформаційної безпеки Виконавчого комітету Бориспільської міської ради

З метою підвищення рівня інформаційної безпеки, забезпечення кіберзахисту інформаційно-комунікаційних систем Виконавчого комітету Бориспільської міської ради, своєчасного виявлення та реагування на кіберзагрози, відповідно до Законів України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», Указу Президента України від 26.08.2021 № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України», п. 20 ч. 4 ст. 42 Закону України «Про місцеве самоврядування в Україні» ЗОБОВ'ЯЗУЮ:

1. Затвердити Політику інформаційної безпеки Виконавчого комітету Бориспільської міської ради (додається).

2. Встановити, що Політика інформаційної безпеки Виконавчого комітету Бориспільської міської ради є обов'язковою до виконання посадовими особами Виконавчого комітету Бориспільської міської ради, які працюють з інформаційними ресурсами.

3. Керівникам виконавчих органів, комунальних підприємств та установ міської ради призначити відповідальних осіб з питань інформаційної безпеки та кіберзахисту та затвердити Політики інформаційної безпеки.

4. Контроль за виконанням цього розпорядження покласти на керуючого справами Лещенка С.О.

Секретар міської ради **Владислав БАЙЧАС**

ЗАТВЕРДЖЕНО
Розпорядження голови
21.11.2025 № 153

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Виконавчого комітету Бориспільської міської ради

Зміст

1. Загальні положення

Політика інформаційної безпеки Виконавчого комітету Бориспільської міської ради (далі – Політика) визначає загальні вимоги до інформаційної безпеки у Виконавчому комітеті Бориспільської міської ради (далі – Установа), основні принципи, цілі та завдання управління інформаційною безпекою.

Політика є обов'язковим документом для ознайомлення при прийомі на роботу та являється доступною для ознайомлення будь-якому співробітникові Установи або третій стороні.

Політика є офіційно прийнятою Керівництвом Установи системою поглядів на проблеми забезпечення інформаційної безпеки, встановлює принципи побудови процесів управління інформаційною безпекою на основі систематизованої розробки та впровадження політик, положень, регламентів, стандартів, інструкцій та інших нормативних документів в області інформаційної безпеки.

Метою Політики є:

забезпечення захисту інформаційних ресурсів Установи від зовнішніх і внутрішніх загроз;

безперервність роботи всіх служб і сервісів Установи;

мінімізація ризиків операційної діяльності Установи;

створення позитивної репутації Установи при взаємодії з третіми сторонами;

відповідність законодавству України та вимогам контролюючих органів в області інформаційної безпеки та захисту персональних даних.

Політика поширюється на всі процеси діяльності Установи та є обов'язковою для виконання всіма співробітниками. Порушення вимог Політики тягне за собою дисциплінарну відповідальність та відповідальність згідно з чинним законодавством України.

2. Терміни та визначення

Власник ІА – співробітник Установи, який несе відповідальність за: забезпечення належної класифікації інформації та активів, пов'язаних із засобами обробки інформації; визначення та періодичний перегляд обмежень доступу і класифікацій; управління конкретними ризиками, пов'язаними з активом, і визначення пов'язаних потреб в безпеці.

Внутрішній аудит – аудит інформаційної безпеки, що проводиться співробітниками Установи, відповідно навченими та незалежним від контролюючої особи.

Вплив – величина збитку, який можна очікувати в результаті наслідків несанкціонованого розкриття інформації, несанкціонованої зміни інформації,

несанкціонованого знищення інформації або втрати інформації або порушення доступності інформаційної системи.

Доступність – властивість інформації, яка полягає в тому, щоб бути доступною та використовуватися на вимогу користувача і/або процесу.

Загроза – можлива небезпека, яка може використовувати уразливість в інформаційній системі для порушення цілісності, конфіденційності, доступності системи.

Інформаційна безпека (ІБ) – це практика забезпечення захисту інформаційних активів від загроз, які можуть на них вплинути. Вона включає в себе вичерпний набір засобів управління, які охоплюють різні фактори (людські, фізичні, екологічні та технічні) протягом життєвого циклу інформаційних і технологічних активів, включаючи розробку, створення і впровадження нових систем, підтримка даних і систем, моніторинг використання таких активів, виявлення та реагування на потенційні загрози, дотримання чинних законів і положень про кібербезпеку і конфіденційність, а також виведення з експлуатації ІТ-систем і знищення даних.

Інформаційна система – комп'ютерні системи, програмне забезпечення, телекомунікаційне і периферійне устаткування.

Інформаційний актив (ІА) – обладнання, програмне забезпечення, дані, а також співробітники, які беруть участь в процесах діяльності Установи, які визначені і управляються як єдине ціле, щоб його можна було зрозуміти, спільно використовувати, захищати та ефективно керувати. Інформаційні активи мають керовану цінність, ризики, контент і життєві цикли.

Інцидент – це подія, яка не є частиною звичайних операцій і порушує робочі процеси. Інцидент може включати відмову функції або послуги, які повинні були бути надані, або будь-які інші типи збою операції.

Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом.

Користувач – особа або Установа, які взаємодіють з інформаційними системами.

Оцінка ризиків – процес виявлення, визначення пріоритетів та аналіз ризиків. Процес включає визначення ступеня, в якому несприятливі обставини або події можуть вплинути на Установу. Цей процес використовує результати оцінок загроз і вразливостей для виявлення ризиків для діяльності Установи і оцінює ці ризики, з точки зору ймовірності виникнення і впливу. Результатом оцінки ризику є список передбачуваних потенційних впливів і явних вразливостей. Оцінка ризиків є частиною процесу управління ризиками.

Політика інформаційної безпеки – набір задокументованих управлінських рішень, створений для захисту інформації Установи та пов'язаних з нею ресурсів.

Ризик – ймовірність впливу на діяльність Установи (включаючи місію, функції, імідж, репутацію), її активи (ресурси) і співробітників в результаті експлуатації вразливостей інформаційної системи і залежно від потенційного впливу, реалізація загрози і ймовірність її реалізації.

Уразливість – недолік в інформаційній системі, який може бути використаний суб'єктом загрози (наприклад, зловмисником) для виконання несанкціонованих дій в системі і порушення цілісності, конфіденційності, доступності або спостережливості.

Цілісність – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом.

Шифрування – процес перетворення відкритого тексту в зашифрований з метою безпеки або конфіденційності.

Шкідливе ПЗ – програмне забезпечення, яке вживлюється в систему, як правило, таємно, з метою порушення конфіденційності, цілісності та/або доступності даних, додатків або операційної системи користувача або іншим чином шкодити або заважати роботі користувача.

SMTPS – Simple Mail Transfer Protocol Secure.

3. Політика інформаційної безпеки

3.1. Управління інформаційною безпекою

Для забезпечення ІБ, необхідно слідувати формальним загальним правилам та процедурам наведеним далі, що покривають відповідне використання ІА Установи.

Співробітники Установи та відповідні треті сторони (які мають доступ до інформації та/або ресурсів Установи) повинні бути проінформовані про необхідність дотримання цієї Політики.

Для забезпечення постійної придатності, адекватності та ефективності ця Політика повинна переглядатися Відповідальною особою за інформаційну безпеку через заплановані проміжки часу – щонайменше раз в рік, якщо впроваджуються суттєві зміни або за рішенням Керівництва Установи.

Суттєвими змінами можна вважати:

зміни в процесах діяльності Установи;

зміни в організаційній структурі;

зміни в ІТ-інфраструктурі Установи тощо.

Відповідно до сфери діяльності Установи необхідно також враховувати наступні моменти:

законодавство, що регулює сферу діяльності Установи та договірні зобов’язання;

відповідальність за порушення Політики;

обов’язки керівництва Установи та інших осіб щодо безпеки систем та інформації Установи.

3.2. Розподіл обов’язків з інформаційної безпеки

Загальна відповідальність за ІБ Установи покладається на міського голову.

Конфліктні обов’язки та сфери відповідальності повинні бути розділені, щоб зменшити можливості для несанкціонованих або ненавмисних змін чи зловживання ІА Установи.

Формальне розподілення відповідальності керівництвом Установи забезпечує стратегічну прозорість та вплив на практику забезпечення ІБ.

Керівництво відповідальне за:

визначення критичних операційних процесів для діяльності Установи;

прийняття рішень щодо розвитку ІБ Установи;

затвердження та поширення правил і вимог ІБ в Установі;

затвердження відповідальності за порушення правил та вимог ІБ;

функцію перевірки та контролю виконання в Установі правил та вимог ІБ.

Додатково відповідальні та їх обов'язки описані нижче в тілі цієї Політики.

3.3. Безпека людських ресурсів

Перевірка кандидатів перед працевлаштуванням, співробітників чи третіх сторін повинна чітко враховувати чутливість інформації, до якої кандидати отримають доступ, та передбачувані ризики при визначенні характеру та строків цих перевірок.

Призначення на посади та звільнення з посад повинно виконуватися відповідно до державних нормативно-правових актів.

Кожен співробітник Установи та третьої сторони, якому надано доступ до систем та/або даних Установи, несе відповідальність за безпечне використання систем і даних для цілей діяльності ТГ та дотримання її політик.

Співробітники та треті сторони несуть відповідальність за повідомлення Керівнику про будь-які сумніви щодо ефективності процесів безпеки, про будь-яку подію чи інцидент щодо несанкціонованого або неправильного використання активів Установи.

Обов’язок Керівництва Установи вимагати від всіх співробітників та третіх сторін дотримання вимог ІБ Установи, відповідно до встановлених політик та процесів, а також контролювати процес їх дотримання.

Припинення трудової діяльності здійснюється згідно з чинним трудовим законодавством України.

3.4. Навчання та обізнаність

Усі співробітники, які є користувачами внутрішньої мережі повинні бути ознайомлені з внутрішніми вимогами щодо роботи з інформаційними активами Установи та нести персональну відповідальність за їх дотримання.

Усі співробітники та відповідні треті сторони повинні проходити відповідну підготовку з підвищення обізнаності та регулярно отримувати інформацію про оновлення організаційних політик та процедур відповідно до їх робочих функцій.

Програма обізнаності повинна забезпечувати, щоб усі співробітники досягали та підтримували принаймні базовий рівень розуміння питань ІБ, таких як загальні зобов'язання згідно з різними політиками, стандартами, процедурами, керівними принципами, законами, нормативними актами, контрактними умовами, а також загальноприйнятими стандартами етики та прийнятної поведінки.

Додаткове навчання підходить для співробітників, які мають конкретні зобов'язання щодо захисту інформації та кому не вистачає базової обізнаності щодо ІБ в рамках робочого процесу, наприклад, адміністраторам систем, відповідальним за ІБ, Керівництву Установи. Такі вимоги до навчання повинні бути визначені в особистих планах навчання співробітників.

3.5. Фізична безпека

Засоби обробки інформації повинні розміщуватися в захищених зонах, фізично захищених від несанкціонованого доступу, пошкодження та втручання чи зміни певних периметрів безпеки. Для виявлення або запобігання несанкціонованого доступу та захисту ІА, особливо критичних і чутливих, повинні застосовуються багаторівневі внутрішні та зовнішні засоби контролю від примусових або прихованих атак.

Співробітники та треті сторони повинні використовувати фізичний ідентифікатор контролю доступу (картка або будь-яка інша альтернатива), щоб мати доступ до приміщень Установи. Для входу в зони обмеженого доступу (серверні, фінансовий відділ тощо) співробітники/третя сторона повинні мати відповідний рівень доступу. Цей рівень затверджується Керівництвом Установи.

Відвідувачі Установи повинні завжди супроводжуватись відповідальними співробітниками задля уникнення доступу до ІА Установи, що можуть містити чутливу інформацію.

Ідентифікатори доступу мають видаватися під час адаптації співробітників в Установі та знищуватися, коли співробітник залишає Організацію.

3.6. Класифікація та управління інформацією

Інформацію слід класифікувати, визначати та оцінювати ризики відповідно до її конфіденційності, цілісності, доступності та спостережливості, незалежно від носія, на якому вона зберігається і/або обробляється. Чутлива інформація повинна визначатися відповідно до її конфіденційності, цілісності, доступності та спостережливості. Вся інформація, окрім публічної, має визначатися як чутлива.

Незалежно від рівня конфіденційності, вся інформація Установи повинна використовуватися належним чином та тільки для дозволених цілей.

Розкриття інформації з обмеженим доступом може здійснюватися лише у законний спосіб зацікавленим особам органів влади, а також фізичним та

юридичним особам за згодою Установи, з дотриманням вимог чинного законодавства України та вимог відповідних Договорів.

3.7. Обробка, передача та зберігання даних

Чутливі дані повинні збиратися та зберігатися лише в системах, де є обґрунтована ділова чи технічна потреба. Чутливі виробничі дані повинні бути захищені при зберіганні і/або використанні у системах, і надійно видалятись, коли вони більше не потрібні.

Діаграма або схема потоків даних повинна бути впровадженою та регулярно переглядатись. Інвентаризація та класифікація даних повинна проводитися щонайменше раз на рік.

Чутливі дані ніколи не повинні збиратися або використовуватися для цілей, відмінних від тих, для яких дані були зібрані спочатку. Усі параметри збереження даних (періоди, цілі тощо) повинні бути законними та відповідати місцевому та міжнародному законодавству та нормам щодо захисту даних.

Інвентаризація чутливих даних повинна включати ідентифікацію конкретних захоплених елементів даних, де дозволено зберігання кожного елементу і необхідних заходів безпеки – наприклад, для захисту конфіденційності та/або цілісності – для кожного елемента даних під час зберігання і передачі.

У разі збору або зберігання чутливих виробничих даних, вони повинні бути належним чином захищені – наприклад, за допомогою надійних заходів контролю доступу та/або надійної криптографії з прийнятими в галузі ІБ процесами управління ключами. Як тільки вони більше не потрібні для цілей збору, дані повинні бути надійно видалені, щоб було неможливо відновити або переробити дані з будь-якої системи.

3.8. Управління інформаційними активами

Усі інформаційні активи Установи повинні бути визначені та задокументовані в Реєстрі ІА. ІА Установи можуть включати:

інформацію про Установу та зацікавлені треті сторони (підрядники, партнери, клієнти тощо),

системи, послуги чи обладнання, в яких обробляється, зберігається або передається інформація про Установу та зацікавлених третіх сторін.

Установа має регулярно переглядати та призначати відповідні обов’язки з обслуговування та перевірки Реєстру ІА. Реєстр повинен містити інформацію про:

власників ІА;

назви ІА;

рівень критичності ІА.

Власник ІА не несе фінансову відповідальність за актив, а відповідає за забезпечення конфіденційності, цілісності, доступності та спостережливості ІА. Власники ІА повинні нести основну відповідальність і відповідати за належний контроль доступу до своїх активів.

Критерії класифікації активів та виявлення критично важливих активів для діяльності Установи – тих активів, порушення конфіденційності, цілісності, доступності або спостережливості яких може суттєво вплинути на діяльність Установи, повинні бути визначені та встановлені. ІА можуть бути класифіковані за рівнем критичності для Установи, відповідно до внутрішніх її вимог.

Ролі та обов'язки повинні бути визначені для Власників ІА та користувачів ІА.

3.9. Використання особистих пристроїв

Установа може дозволяти співробітникам та іншим авторизованим користувачам своїх систем, послуг та ресурсів використовувати власні пристрої для виконання посадових обов'язків та завдань, які необхідні для забезпечення її безперервної діяльності.

Установа повинна розробити та встановити вимоги ІБ щодо використання власних робочих пристроїв та довести їх до відома усіх співробітників та відповідних третіх сторін. Особисту відповідальність має нести кожен співробітник та третя сторона, що використовує персональний пристрій для доступу до систем, послуг та ресурсів Установи, щоб забезпечити відповідне використання всіх протоколів безпеки та усіх заходів безпеки.

Кожен пристрій, який використовується для виконання посадових обов'язків та завдань, які необхідні для забезпечення безперервної діяльності Установи, тобто для доступу до внутрішньої інформації, повинен використовуватися відповідально та лише в робочих цілях. Невиконання даного правила несе за собою негайне припинення облікового запису користувача.

3.10. Управління доступом

Права доступу повинні бути визначені відповідно до ролей, встановлених в Установі, для того, щоб спростити адміністрування.

Доступ до ІА повинен забезпечуватись відповідно до принципу мінімальних привілеїв (доступ надається тільки до тих систем, які необхідні користувачу в межах роботи) та постійно контролюватися.

Відповідальність за розподіл ролей користувачам та періодичні перевірки повинна бути покладена на Відповідальну особу за ІБ.

Матриця доступу повинна бути визначена для кожної інформаційної системи і надавати інформацію про всі права доступу, надані користувачам до інформації/систем/послуг Установи, із зазначенням рівня доступу: перегляд, редагування, адміністрування.

Легенда Матриці доступу повинна бути встановлена та задокументована, тобто, визначений рівень повноважень, з якими користувач отримує доступ до ресурсу (наприклад, A – адміністратор, E – редактор, R – читання/коментування, V – перегляд).

Усі запити на доступ повинні бути схвалені безпосереднім Керівником співробітника та Відповідальною особою за ІБ перед наданням доступу.

Облікові записи користувачів повинні негайно блокуватися адміністратором систем, якщо до них отриманий несанкціонований доступ або виявлена підозріла активність.

Користування двофакторною аутентифікацією користувачами в тих системах та сервісах, де це можливо, є обов'язковим.

Перегляд користувацьких прав

Відповідальна особа за ІБ повинна регулярно переглядати права доступу користувачів.

Обов'язковим є створення та забезпечення виконання планів перегляду доступів для всіх систем та ІА, особливо критичних. Потрібно враховувати наступне:

права користувачів повинні переглядатися регулярно та після внесення змін, таких як зміна посади або звільнення;

права користувачів повинні переглядатися у разі зміни ролі користувача в Установі;

привілейовані права повинні переглядатися частіше;

привілейовані права доступу повинні регулярно переглядатися, щоб гарантувати, що ніхто не отримував привілейований доступ несанкціонованим способом.

Доступ до мережі та мережевих сервісів

Користувачам повинен надаватися доступ до мережі та мережевих послуг, у разі необхідності такого доступу.

Повинен бути встановлений контроль за переглядом та управлінням доступу, включаючи контроль та впровадження наступних засобів та інструментів:

перелік мереж та мережевих послуг з дозволеним доступом;

процедури визначення необхідного доступу та відповідних користувачів;

інструменти для управління мережевими з'єднаннями та послугами;

засоби та інструменти моніторингу використання мережевих послуг.

3.11. Парольна політика

Відповідно до Парольної політики, для забезпечення надійного захисту інформаційних систем паролем, мають бути встановлені наступні параметри:

мінімальна довжина: 8-12 символів;

пароль повинен відповідати вимогам складності: так;

повинен містити символи верхнього та нижнього регістру, числа, а також неалфавітні символи;

не використовувати будь-які персональні дані;

не містить у собі загальновживані слова;

мінімальний термін дії пароля: 1 день;

максимальний термін дії пароля: 30-90 днів;

зберігати паролі за допомогою оборотного шифрування: ні;

сповіщення про зміну: за 7 днів до закінчення терміну дії;

історія паролів: 10 останніх використаних паролів;

поріг блокування облікового запису: 5 послідовних невдалих спроб введення;

скинути лічильник блокування облікового запису через: 15 хвилин;

безпечне зберігання паролів: паролі не слід зберігати або передавати у відкритому тексті.

3.12. Використання електронної пошти

Доступ до електронної пошти надається співробітникам Установи для виконання своїх службових обов'язків. Використання електронної пошти співробітниками Установи в особистих або інших цілях, не пов’язаних з діяльністю Установи, заборонено.

В Установі заборонено:

надсилати повідомлення, що містять чутливу інформацію, а також дані, що містять чутливу інформацію не для виконання своїх службових обов'язків. Забороняється надсилати по електронній пошті логіни, паролі та іншу чутливу інформацію;

використовувати електронну пошту для особистих цілей;

використовувати електронну адресу для підписки на маркетингові електронні листи без попереднього узгодження з Відповідальною особою за ІБ;

відкривати будь-яке вкладення, посилання чи додаток до електронної пошти, де співробітник не має ґрунтовних підстав вважати, що інформація, до якої очікується доступ, надійшла з надійного джерела;

надсилати масові розсилки (понад 10) на зовнішні адреси без згоди Керівника співробітника та Відповідальної особи за ІБ;

надсилати по електронній пошті матеріали, що містять шкідливе програмне забезпечення чи інші програми, призначені для порушення, знищення або обмеження функціональних можливостей будь-якого комп’ютерного чи телекомунікаційного обладнання чи інформаційних систем та послуг;

надсилати електронною поштою програми, які забезпечують несанкціонований доступ;

розповсюджувати за допомогою електронної пошти матеріали, які захищені авторським правом і зачіпають будь-який патент, торгову марку, комерційну таємницю, авторські права або будь-які інші права власності. та/або авторські права або пов’язані з ними права третіх сторін;

поширювати через електронну пошту інформацію, заборонену міжнародним та українським законодавством, включаючи матеріали, що є шкідливими, загрозливими, нецензурними, а також інформацію, що порушує честь та гідність інших. Також забороняється надсилати матеріали, що розпалюють національну ворожнечу, підбурюють до насильства, закликають до незаконних дій, включаючи

матеріали, що містять інструкції щодо використання вибухових речовин, зброї тощо.

Доступ колишнього співробітника до облікових записів електронної пошти ТГ повинен бути негайно відключений та деактивований.

3.13. Безпека мережі

Наступні вимоги обов'язкові до виконання:

вимоги до конфігурації безпеки повинні бути визначені для всього мережевого обладнання;

вимоги до контролю аутентифікації та доступу повинні бути визначені та повинні бути впроваджені;

вимоги до систем та механізмів моніторингу безпеки мережі повинні бути визначені, впровадженні, необхідним чином управлятися;

усі оновлення повинні вчасно встановлюватись;

зміни можуть бути внесені лише адміністратором систем або відповідним авторизованим користувачем;

процес резервного копіювання мережевих пристроїв (наприклад, системного програмного забезпечення, даних конфігурацій, файлів баз даних) повинен відбуватися регулярно;

вимоги до конфігурування безпеки Wi-Fi мереж:

- зміна паролів за замовчуванням;
- вимкнення WPS;
- вимкнення SSID Broadcast;
- своєчасне оновлення прошивки;
- обмеження можливості під'єднання пристроїв до локальної мережі.

Протоколи безпечного зв'язку

Щоб захистити інформацію в системах та додатках Установи, необхідно належним чином управляти та контролювати мережі.

Використання протоколів безпечного зв'язку гарантують конфіденційність, цілісність, доступність та спостережливості інформації, що передається. Наступні протоколи найбільш прийнятні для використання:

- SSH2;
- SFTP;
- TLS 1.2-1.3;
- HTTPS;
- WSS;
- SMTPS;
- DNS-over-HTTPS.

3.14. Використання робочих пристроїв

ТГ повинна встановити вимоги щодо безпеки пристроїв, змінних носіїв під час їх використання.

Робочі пристрої користувачів в Установі мають контролюватися централізованою системою управління.

Обов'язкове блокування екрану на пристроях після встановленого часу бездіяльності повинне бути налаштоване на всіх робочих пристроях.

Захист робочих пристроїв шляхом шифрування жорстких дисків та паролів для розблокування повинен бути реалізованим за необхідності.

Персонал несе відповідальність за забезпечення фізичної безпеки робочих пристроїв при їх використанні за межами приміщень Установи (обмеження фізичного доступу третіх сторін, слідування вимогам блокування екрану).

Забезпечення виконання вимог щодо безпечного використання робочих пристроїв має бути автоматизовано за допомогою відповідних програмних інструментів. Політики налаштування таких інструментів повинні регулярно переглядатись на відповідність даній Політиці та іншим цільовим політикам Установи.

3.15. Встановлення безпечних оновлень

Установа повинна встановити вимоги щодо встановлення оновлень на всіх ІА, з яких надається доступ до інформації/послуг/ресурсів Установи.

Режим автоматичного оновлення виправлень або можливість зробити це вручну має бути забезпечена адміністратором систем. Антивірусне програмне забезпечення та інші компоненти безпеки повинні регулярно перевірятись та оновлюватись до останньої версії.

Перед встановленням оновлень на виробничі системи необхідно проводити тестування оновлень в окремому тестовому середовищі.

Установа повинна проводити періодичний огляд на веб-сайті постачальника, який надає інформаційні активи на наявність оновлень.

Якщо операційна система – Windows, інструмент управління виправленнями повинен бути налаштований таким чином, щоб він автоматично завантажував останні виправлення безпеки Microsoft. Перевірка та застосування виправлень повинна проводитись за необхідності.

Системи Linux повинні своєчасно оновлюватися відповідними патчами, протестованими та впровадженими належним чином.

Адміністратор систем відповідальний за затвердження всіх виправлень та відповідальний за всі технічні зміни конфігурацій та операційних систем, програмного забезпечення, антивірусних оновлень, своєчасного встановлення виправлень та драйверів для мережевих пристроїв, робочих станцій.

3.16. Обмеження встановлення програмного забезпечення

Правила до встановлення програмного забезпечення користувачами повинні бути визначені та впроваджені Установою.

Установа повинна створити та застосовувати правила щодо дозволеного для встановлення програмного забезпечення та контролю, базуючись на принципі мінімальних привілеїв. Відповідальна особа за ІБ та адміністратор систем мають

створити списки дозволеного та забороненого для встановлення програмне забезпечення.

Встановлення програмного забезпечення повинно бути обмежене для всіх користувачів, проте можливі винятки, які повинні бути схвалені адміністратором систем та Відповідальною особою за ІБ.

Функція контролю закріплена за Відповідальною особою за ІБ та Керівництвом, щоб забезпечити належний рівень контролю та розділення привілеїв.

3.17. Захист від шкідливого ПЗ

Попереднє тестування програмного забезпечення та перевірка файлів до їх встановлення на пристроях, з яких існує доступ до корпоративної інформації/систем/ресурсів повинні забезпечуватись адміністратором систем.

Лише програмне забезпечення, затверджене адміністратором систем та Відповідальною особою за ІБ, дозволено встановлювати на системи Установи.

Сканери проти шкідливого ПЗ необхідно налаштувати на автоматичне сканування відповідних компонентів відразу після випуску оновлень.

Установа має налаштувати антивірусне програмне забезпечення на: сканування під час завантаження, сканування файлових та поштових серверів принаймні один раз на день та будь-яких інших серверів – принаймні раз на тиждень, сканування файлів при відкритті, сканування вкладень вхідної та вихідної електронної пошти, веб сканування вмісту при синхронізації із скануванням портативних пристроїв, де це можливо.

Управління та перегляд журналів антивірусного програмного забезпечення має здійснюватися адміністратором систем.

Для захисту програмного забезпечення від шкідливих програм Установи повинно здійснюватися: ручне/автоматичне та планове сканування, видалення заражених файлів, розміщення заражених файлів на карантин, які неможливо видалити, можливість автоматичного та запланованого оновлення, реєстрація випадків шкідливого програмного забезпечення та забезпечення можливості аналізу логів, централізоване управління та ведення логів.

Комп’ютери, у яких виявлено шкідливе програмне забезпечення, та комп’ютери без антивірусного програмного забезпечення заборонено під’єднувати до внутрішньої мережі Установи.

Адміністратор систем повинен періодично перевіряти на веб-сайті постачальника інформаційних активів на наявність відповідних оновлень. Адміністратор систем має налаштовувати режим автоматичного оновлення патчів або робити це вручну.

Відповідальність за контроль дотримання захисту від шкідливого ПЗ покладено на Відповідальну особу за ІБ.

3.18. Управління потужностями

Установа повинна відстежувати, налаштовувати використання ресурсів та складати прогнози щодо майбутніх вимог до потужності, щоб забезпечити необхідну продуктивність систем.

Відповідальними співробітниками Установи має проводитись регулярно аудит потужностей. Вимоги до нього повинні бути визначені відповідно до пріоритету інформаційної системи для діяльності Установи.

Особливу увагу слід приділити дороговартісним ресурсам , або таким, що потребують багато часу на отримання/відновлення. Адміністратор систем та Відповідальна особа за ІБ несуть відповідальність за моніторинг ключових показників ефективності систем.

3.19. Логування та моніторинг

Інформація, яку слід збирати з власних систем має включати в себе:

дату та час події;

ідентифікатор користувача;

тип запиту/дії;

статус запиту (успішний чи невдалий);

події, що включають зміни, можуть вказувати на початок та кінцевий стан тощо.

Установа повинна визначити необхідність проведення ручного збору логів в тих системах, де це неможливо автоматично або, якщо автоматичний аудит логів не містить необхідної інформації.

Для реалізації неможливості зміни/видалення журналів логів адміністратором систем, в Установі мають бути впроваджені додаткові засоби контролю та рішення для реєстрації дій. Якщо критично важливі системи не мають функції реєстрації дій адміністратора систем, потрібно перейти на версії або нові платформи з наявною такою функцією або здійснити затвердження таких винятків Керівництвом Установи. У разі неможливості зміни систем чи сервісів, такі винятки повинні бути погоджені з Керівництвом.

Установа має вживати організаційних заходів та впроваджувати інструменти захисту для сховища з архівом логів.

3.20. Віддалений доступ

Інтернет-ресурси Установи мають використовуватися для дистанційного виконання робочих завдань, інформаційно-аналітичної роботи в інтересах Установи, обміну поштою із третіми сторонами.

Інше використання Інтернет-ресурсів слід розглядати як порушення.

Підключення до мережі Інтернет в Установі повинно здійснюватися адміністратором систем у порядку надання прав доступу. При переміщенні співробітника (звільненні, переведенні в інший підрозділ) його безпосередній Керівник повинен подати заяву на скасування прав доступу.

Віддалене підключення до інформаційних активів Установи має здійснюватися за допомогою визначених адміністратором систем та Відповідальною особою за ІБ ресурсів.

З'єднання веб-зустрічей/віддаленого управління (наприклад, TeamViewer, AnyDesk) не повинні використовуватися в мережі Установи для надання віддаленого доступу третім сторонам за замовчуванням. Цей тип підключень дозволений лише для технічного обслуговування та усунення несправностей систем після належної авторизації.

3.21. Резервне копіювання

Резервне копіювання повинно здійснюватися регулярно.

Критично важлива інформація, програмне забезпечення та системи, що підлягають резервному копіюванню, повинні бути визначені.

Періодичність створення резервних копій та частота їх тестування повинні бути чітко визначені.

Тип резервного копіювання (повне, інкрементне, диференційоване) повинен бути визначений адміністратором систем для кожної системи.

Резервні копії повинні зберігатися окремо від основних копій та повинен бути забезпечений належний рівень безпеки, а доступ до резервних копій повинен бути обмежений на тому ж рівні, що і для основних копій.

Доступ до резервних копій повинні мати лише визначені співробітники Установи.

Відповідальність за здійснення резервного копіювання покладається на Відповідальну особу за ІБ.

3.22. Безпека комунікацій

Установа повинна визначити дозволені методи для зв'язку (передачі корпоративної інформації) всередині Установи та з третіми сторонами.

Обов'язковою є перевірка вкладень з поштових скриньок та інших месенджерів перед завантаженням.

Заборонений доступ до ресурсів Установи за прямим посиланням.

Під час обміну інформацією повинні використовуватись лише захищені протоколи передачі даних.

В Установі повинен бути впроваджений та підтримуватись процес електронного спілкування, включаючи питання безпеки, відповідно до рівня конфіденційності переданої інформації. Там, де це необхідно, повинні бути впроваджені додаткові засоби захисту (цифровий підпис, шифрування тощо).

3.23. Управління змінами

Установа повинна контролювати зміни в процесах діяльності, засобах обробки інформації та системах, що впливають на ІБ.

Процедури управління змінами повинні включати:

ідентифікацію та реєстрацію суттєвих змін;

планування та тестування змін;

аналіз потенційного впливу (включаючи ІБ);

відповідність вимогам ІБ;

процедури затвердження змін;

процедури відкату;

процедура реалізації термінових змін для швидкого та контрольованого виконання змін у разі реагування на аварії та дій відновлення.

3.24. Управління вразливостями

Інформацію про технічні вразливості використовуваних інформаційних систем слід отримувати своєчасно, оцінювати їх вплив та вживати відповідних заходів для усунення пов'язаного з цим ризику.

Оцінка вразливостей повинна проводитись регулярно та бути частиною процесу управління вразливостями. Для критичних систем та зовнішньої/внутрішньої мережі, тестування на проникнення периметру повинно проводитися періодично. Відповідальність за контроль проведення оцінки вразливостей покладено на третю сторону, а усунення вразливостей покладено на адміністратора систем та/або Відповідального співробітника за інформаційну безпеку.

3.25. Управління ризиками

Управління ризиками є невід'ємною частиною діяльності на всіх рівнях Установи. Метою управління ризиками є надання Керівництву Установи інформації, необхідної для прийняття обґрунтованих рішень щодо зміни пріоритетів діяльності для управління областями неприйнятно високого ризику.

Установа має здійснювати оцінку ризиків, оскільки це процес ідентифікації, вимірювань та визначення пріоритетів ризиків ІБ.

Установа має впровадити відповідні заходи безпеки для мінімізації ризиків після проведення оцінки та їх пріоритезації.

Процес оцінки та управління ризиками ІБ має бути інтегрований в процес управління ризиками діяльності.

3.26. Управління інцидентами

Установа повинна регулярно проводити навчання та підвищення обізнаності персоналу в сфері управління інцидентами. Підтримувати та розвивати процес реагування на всі типи інцидентів ІБ, відповідно до Політики реагування на інциденти кібербезпеки (додаток 1).

Установа повинна підтримувати План реагування на інциденти кібербезпеки (додаток 2), який повинен спиратися на постійний оперативний моніторинг і процедури реагування на інциденти.

Кожен співробітник несе відповідальність за повідомлення Відповідальної особи за ІБ, коли він або вона дізнаються про те, що стався або міг статися інцидент ІБ, який міг поставити під загрозу безперервність діяльності Установи.

Співробітники та треті сторони можуть намагатися вирішити інциденти ІБ лише за вказівками та з прямого дозволу Відповідальної особи за ІБ.

З міркувань безпеки та технічних міркувань Установи залишає за собою право відстежувати, записувати та реєструвати все використання своїх інформаційних активів і діяльність у мережі Установи.

3.27. Безперервність діяльності

Установа повинна забезпечити наявність необхідних ресурсів для безперервної діяльності та швидкого відновлення критичних систем у разі непередбачуваних ситуацій.

Керівники підрозділів несуть відповідальність за визначення вимог щодо захисту доступності систем/сервісів/даних і несуть остаточну відповідальність за їх виконання. Вимоги мають базуватися на аналізі ризиків, критичності активів і враховувати нормативні вимоги. Керівництво несе відповідальність за забезпечення необхідного фінансування для їх реалізації. Відповідальна особа за ІБ повинен забезпечувати та підтримувати безперервність систем на випадок непередбачених обставин.

Можливості аварійного відновлення особливо вразливі до збоїв і не повинні вважатися прийнятними, якщо вони не проходять регулярні задокументовані випробування.

4. Перелік відповідальних осіб

Роль	ПІБ
Відповідальна особа за інформаційну безпеку	Начальник відділу експлуатації та підтримки інформаційно-телекомунікаційної інфраструктури
Адміністратор систем	Головний спеціаліст відділу експлуатації та підтримки інформаційно-телекомунікаційної інфраструктури
Треті сторони	Представники технічної підтримки
Керівництво	Заступники міського голови або керуючий справами виконавчого комітету міської ради відповідно до розподілу обов’язків

Додаток 1
до Політики

Політика управління інцидентами кібербезпеки

1. Загальне

Політика управління інцидентами кібербезпеки (далі – ПУ) визначає вимоги та послідовність дій щодо виявлення, аналізу та опрацювання інцидентів кібербезпеки (далі – КБ) у виконавчому комітеті Бориспільської міської ради (далі – Установа).

Метою ПУ є забезпечення:

організація оперативного виявлення, оцінки та реагування на інциденти КБ;

мінімізації наслідків інцидентів КБ;

запобігання інцидентам КБ в майбутньому, поліпшення впровадження та використання захисних заходів КБ;

відповідності рівня КБ Установи вимогам законів України, нормативно-правових актів України та міжнародних стандартів в області КБ;

захисту інформаційних систем Установи від порушень конфіденційності, цілісності, доступності та спостережності.

1.1. Класифікація інцидентів

За наслідками інциденти КБ повинні класифікуватись за відповідно до таблиці, яка наведена у **пункті 2.2.3** цієї ПУ.

1.2. Види інцидентів

В цій Політиці визначені наступні види інцидентів:

порушення цілісності інформації;

порушення конфіденційності;

порушення доступності;

порушення спостережності.

2. Реагування на інциденти КБ

Етап реагування на інциденти КБ в інформаційних системах Установи повинен включати наступні кроки:

Підготовка;

Виявлення та аналіз;

Стримування;

Усунення;

Відновлення;

Аналіз ефективності.

2.1. Підготовка

Для забезпечення готовності Установи до оперативного реагування на інциденти КБ повинні бути розроблені плани реагування на окремі види інцидентів КБ, що є найбільш ймовірними для певної прикладної системи з урахуванням умов та режиму її функціонування виходячи з прогнозованих даних та експертних оцінок.

Розробка планів реагування на інциденти КБ є основою для системного підходу до процесу управління інцидентами КБ в Установі.

2.1.1. Етап «Створення плану реагування на інцидент КБ»

Відповідальна особа за ІБ повинна проводити пошук інформації про аналогічні інциденти КБ, які відбувалися в минулому та для яких розроблено типовий план реагування.

Якщо для поточного виду інциденту КБ у базі знань існує типовий план реагування, то Відповідальна особа за ІБ переходить до його реалізації.

Якщо подібних інцидентів КБ у базі знань немає, Відповідальна особа за ІБ повинна розробити комплекс заходів, який оформлюється у вигляді плану реагування на інцидент КБ та зберігається в базі знань.

2.2. Виявлення та аналіз

2.2.1. Етапи «Виявлення та інформування про інцидент. Збір та реєстрація інформації про інцидент КБ»

У разі виявлення інциденту або слабких місць КБ працівники Установи або залучені треті сторони повинні повідомити про це Відповідальну особу за ІБ.

До основних ознак інциденту відносяться наступні (невичерпний перелік):

суттєве зниження продуктивності прикладних систем або недоступність прикладних систем;

повідомлення антивірусного ПЗ;

несанкціонована діяльність у мережі та прикладних системах Установи;

стрімке збільшення мережевого трафіку;

численні повідомлення про помилки та збої;

зафіксовані спроби підбору паролів;

заздалегідь відома негативна подія безпеки;

подія безпеки, що зафіксована у неробочий час;

невідомі облікові записи;

відключені засоби забезпечення безпеки;

спроби застосування методів соціальної інженерії;

відсутність засобів захисту інформації та ін;

Працівник Установи, який виявив можливі ознаки інциденту, повинен вказати у повідомленні наступну інформацію:

опис проблеми, що спостерігається;

час виникнення ознак інциденту;

інші суттєві дані щодо інциденту – у відповідь на запитання Відповідальної особи за ІБ

2.2.2. Етап «Аналіз інциденту»

Процедура повинна розпочинатись за фактом отримання Відповідальною особою за ІБ повідомлення про виникнення інциденту КБ.

Після отримання пміського овідомлення про інцидент Відповідальна особа за ІБ повинна провести класифікацію інциденту, аналіз зібраної інформацію та прийняти рішення щодо підтвердження його статусу.

2.2.3. Етап «Оповіщення про інцидент»

В Установі оповіщення зацікавлених сторін (міський голова, заступники голови, Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України, Служба безпеки України, Національний координаційний центр кібербезпеки при РНБО України, залучені треті сторони – відповідно до договірних вимог, тощо) повинно здійснюватися Відповідальною особою за ІБ визначеними засобами після маркування.

Маркування повинно проводитися відповідно до наступних значень:

Мітка (колір)	Значення
рівень 0, некритичний (білий)	Кіберінцидент/кібератака не загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем.
рівень 1, низький (зелений)	Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, але не загрожує захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються.

рівень 2, середній (жовтий)	Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, внаслідок чого створюються передумови для порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються, виникають передумови для припинення виконання функцій та/або надання послуг критичною інфраструктурою.
рівень 3, високий (помаранчевий)	Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають потенційні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою. Реагування на цьому рівні може потребувати залучення сил та засобів більше ніж одного основного суб'єкта національної системи кібербезпеки.

рівень 4, критичний (червоний)	Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування кількох інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають реальні загрози для національної безпеки і оборони, стану навколишнього природного середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою. Кіберінцидент/кібератака може мати транскордонний вплив. Реагування на цьому рівні потребує залучення сил та засобів основних суб'єктів національної системи кібербезпеки.
рівень 5, надзвичайний (чорний)	Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування значної кількості інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають невідворотні загрози для повноцінного функціонування держави або загроза життю громадян України. Кіберінцидент/кібератака може мати транскордонний вплив. Реагування на цьому рівні потребує максимального залучення сил та засобів основних суб'єктів національної системи кібербезпеки та інших суб'єктів забезпечення кібербезпеки.

2.3. Стримування

2.3.1. Етап «Збір інформації для розслідування інциденту»

Відповідальна особа за ІБ відповідно до плану реагування повинна зібрати інформацію про інцидент для проведення подальшого розслідування.

У випадку, коли при реалізації збору інформації про інцидент КБ планується переривання роботи інформаційно-комунікаційної системи (далі ІКС), Відповідальна особа за ІБ, повинна погодити таке переривання з Керівництвом Установи.

2.3.2. Етап «Зменшення впливу інциденту»

Відповідальна особа за ІБ повинна обрати методи та заходи, спрямовані на зменшення впливу інциденту на процеси діяльності Установи, окремо для кожного конкретного інциденту, залежно від його виду, та у відповідності з розробленим, планом реагування.

Будь-які методи, дії та порядок їхнього використання або виконання повинні погоджуватися Керівництвом Установи.

Відповідальна особа за ІБ повинна виконати оцінку можливого впливу запланованих дій на безперервність діяльності ураженої системи та проінформувати Керівництво Установи. За необхідності допускається ізолювання системи або роз'єднання компонентів цієї системи на період проведення повного розслідування інциденту.

2.4. Усунення інциденту та відновлення функціонування інформаційно-комунікаційної системи

З метою відновлення нормального функціонування ІКС Відповідальна особа за ІБ повинна проводити заходи з усунення причин та наслідків інциденту.

Процедура усунення інциденту та відновлення функціонування залежить від виду інциденту та повинна визначатись для кожного інциденту окремо.

Після відновлення функціонування ІКС Відповідальна особа за ІБ має перевірити відсутність ознак повторення інциденту та повідомити про завершення робіт Керівництво Установи.

2.5. Аналіз ефективності заходів з реагування на кіберінциденти/кібератаки

2.5.1. Етап «Розслідування інциденту»

Під час виконання робіт з розслідування інцидентів повинні використовуватись методи та засоби, що запобігають випадковому або навмисному внесенню змін в дані, що вивчаються та аналізуються.

Відповідальна особа за ІБ повинна з'ясувати причини інциденту та провести аналіз усіх виявлених у процесі розслідування небезпечних факторів, що призвели до відхилень:

у діях працівників Установи;

у роботі інформаційних ресурсів та систем;

відхилень від норм експлуатації програмного забезпечення і обладнання;

відхилень від вимог політик ІБ із визначенням ступеня впливу цих відхилень на розвиток інциденту.

Відповідальна особа за ІБ повинна визначити:

які нормативні вимоги були порушені або не виконані (з посиланням на відповідні статті, розділи, пункти нормативних актів);

причетність до інциденту, якщо це мало місце, інших підприємств, організацій і установ із визначенням, наскільки це можливо;

ступеня їх впливу на виникнення і перебіг інциденту.

2.5.2. Етап «Аналіз ефективності»

Після завершення розслідування Відповідальна особа за ІБ повинна підготувати звіт з описом всіх проведених процедур щодо управління інцидентами КБ та закриттям інциденту КБ та надати Керівництву Установи, а також, за необхідності, зацікавленим сторонам.

Відповідальна особа за ІБ повинна внести інформацію про закриття інциденту в журнал реєстрації інцидентів.

3. Система внутрішнього контролю

Всі співробітники Установи несуть відповідальність за своєчасність інформування Відповідальну особу за ІБ у разі виявлення ознак інцидентів КБ або можливості настання інциденту КБ.

Додаток 2
до Політики

План реагування на інциденти кібербезпеки
Опис інциденту кібербезпеки

№	Назва інциденту	План дій щодо реагування на інцидент	Дата/час виконання дій з реагування	Очікувана дата завершення всіх дій з реагування	Технічні, програмні та фінансові ресурси	Місце збереження інформаційних підтверджень та доказів	Відповідальна за реагування особа (ПІБ, Посада)	Статус			Коментарі
								Не розпочато	У процесі	Завершено	

Приклади реагування на інцидент кібербезпеки

Інцидент	Розслідування	Виправлення	Комунікація	Відновлення	Ресурси	Запобігання ризикам
1	2	3	4	5	6	7
Фішинг	Завдання: Визначити та впровадити кроки з розслідування інцидентів КБ, включаючи основні питання та стратегії фішингу. 1. Область та масштаб атаки 2. Аналіз повідомлень 3. Аналіз посилань та вкладень 4. Категоризація типу атак 5. Визначення критичності атаки	Спланувати заходи з усунення інцидентів у яких ці кроки запускаються разом (або скоординовано) з залученням відповідних команд спеціалістів, готових реагувати на будь-які порушення. Визначити необхідний час і компромісні підходи для усунення наслідків. Завдання: Визначити тактичні та стратегічні кроки стримування фішингових атак.	Завдання: Визначити етапи проведення комунікацій під час фішинг атаки. Вказати інструменти та процедуру (зокрема хто повинен бути залучений) для кожного кроку.	Завдання: Визначити кроки відновлення після фішинг атаки. Визначити та вказати інструменти та процедуру для кожного кроку	Приклад: Дії користувача при ймовірній фішинговій атаці Завдання: Визначити кроки для користувачів, які мають підозру на фішинг.	

1	2	3	4	5	6	7
ПРОГРАМИ - ВИМАГАЧІ	Завдання: Визначити та впровадити кроки з розслідування атак/інцидентів, які відбулись за участі програм-вимагачів, зокрема основні питання та стратегії. 1. Визначити тип програм-вимагачів 2. Визначити область застосування 3. Оцінка впливу 4. Знайти інфікованого	Спланувати заходи з усунення інцидентів, у яких ці кроки запускаються разом (або скоординовано) з залученням відповідних команд спеціалістів, готових реагувати на будь-які порушення. Розглянути час і компромісні підходи з усунення інциденту. Завдання: Визначити тактичні та стратегічні кроки стримування програм-вимагачів.	Завдання: Визначити етапи проведення комунікацій. Вказати інструменти та процедуру (зокрема хто повинен бути залучений) для кожного кроку.	Завдання: Визначити кроки відновлення. Визначити та вказати інструменти та процедуру для кожного кроку. Не рекомендовано платити викуп: це не гарантує вирішення проблеми. Все може піти не так (наприклад, помилки можуть зробити дані неможливими для відновлення навіть за допомогою ключа). Крім того, оплата доводить, що програми-вимагачі працюють і можуть посилити атаки проти вас чи будь-кого іншого.	Приклад: Дії користувача при підозрі про наявність програми-вимагача Завдання: Визначити кроки для користувачів, які реагують на наявність програми-вимагача.	

1	2	3	4	5	6	7
АТАКА НА ВЕБСАЙТ	1. Негайно відключити зіпсований сервер для подальшого дослідження. 2. Визначити джерело вразливості системи, яку використав зловмисник. 3. Зібрати будь-які підказки щодо того, ким є хакер або на яку організацію він працює. 4. Зібрати іншу важливу інформацію зі сторінки, яка була зіпсована.	Спланувати заходи з усунення проблем, у яких кроки зі стримування запускаються разом (або скоординовано) з задіянням відповідних команд спеціалістів, готових реагувати на будь-які порушення. Розглянути час і компромісні підходи з усунення інциденту. Завдання: Визначити тактичні та стратегічні кроки стримування пошкодження веб-сайтів	Завдання: Визначити кроки проведення етапу комунікацій. Вказати інструменти та процедуру (зокрема хто повинен бути залучений) для кожного кроку.	Завдання: Визначити кроки відновлення. Визначити та вказати інструменти та процедуру для кожного кроку.	Приклад: Дії користувача при атаці пошкодження веб-сайту Завдання: Визначити кроки для користувачів, які реагують на атаку на веб-сайт.	Завдання: Поспілкуватись з іншими співробітниками, щоб переконатися, що всі розуміють наступні кроки та роблять свій внесок, де це можливо.

1	2	3	4	5	6	7
		1. Створити резервну копію всіх даних, що зберігаються на веб-сервері. 2. Обов'язково тимчасово вимкнути сервер зіпсованої сторінки, поки триває розслідування. 3. Після визначення джерела атаки виконати необхідні кроки, щоб переконатися, що сценарій атаки більше не повториться.				

Інцидент	Підготовка	Розслідування	Аналіз	Виправлення	Відновлення	Після інциденту
1	2	3	4	5	6	7
ВТРАТА ДАНИХ	Забезпечити належний доступ до будь-якої необхідної документації та інформації, включаючи доступ у неробочий час, для наступного: - Процес управління інцидентами; - Схеми архітектури мережі; - Діаграми потоку даних; Визначити та отримати послуги стороннього провайдера.	Завдання: Визначити та впровадити кроки з розслідування, зокрема основні питання та стратегії компрометації, ідентифікації та доступу.	1. Переконатись, що будь-які задіяні дані. 2. Проаналізувати будь-який підозрілий мережевий трафік. 3. Переглянути журнали безпеки та доступу, сканування вразливостей і будь-які автоматизовані результати інструментів. 4. Проаналізувати будь-яку підозрілу активність, файли чи виявлені зразки ЗПЗ.	Етап виправлення: - Містить технічний механізм порушення даних; - Усунення технічного механізму витоку даних; - Відновлення уражених систем і служб та приведення до звичайного стану.	На додаток до загальних кроків і вказівок у плані реагування на інцидент: 1. Відновити системи на основі аналізу впливу на діяльність і критичності діяльності. 2. Здійснити повне антивірусне та розширене сканування шкідливих програм усіх систем по всій організації. 3. Повторно встановити облікові дані всіх задіяних систем і дані	Етап заходів після інциденту має такі цілі: - Заповнити Звіт про інцидент, включаючи всі деталі інциденту та дії. - Завершити процес управління інцидентами. - Опублікувати відповідні внутрішні та зовнішні повідомлення.

1	2	3	4	5	6	7
	Переглянути останні кіберінциденти та їх результати.		5. Зіставити будь-які нещодавні події безпеки або ознаки компрометації з підозрілою активністю в мережі. 6. Визначити джерело компрометації даних. 7. Визначити конкретний набір даних, який було зламано, а також спосіб його зламу. 8. Визначити методологію атаки та графік кіберінцидентів.		облікових записів користувачів. 4. Реінтегрувати раніше скомпрометовані системи. 5. Відновити будь-які пошкоджені або знищені дані. 6. Відновити усі призупинені служби. 7. Встановити моніторинг для виявлення подальшої підозрілої діяльності. 8. Координувати впровадження будь-яких необхідних виправлень або заходів з усунення вразливостей.	