ПЕРЕЯСЛАВСЬКИЙ МІСЬКИЙ ГОЛОВА

Р О З П О Р Я Д Ж Е Н Н Я

від «26» листопада 2025 року № 278/07-04/11-25

Про затвердження Політики інформаційної безпеки структурних підрозділів виконавчого комітету, Переяславської міської ради та плану реагування на кіберінциденти

Із метою забезпечення належного рівня захисту інформаційних ресурсів, підвищення ефективності управління інформаційною безпекою, запобігання загрозам несанкціонованого доступу до інформації; відповідно до Законів України «Про інформацію», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України»; згідно з вимогами ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки», ДСТУ EN ISO/IEC 27701:2022 (EN ISO/IEC 27701:2021, IDT; ISO/IEC 27701:2019, IDT) «Методи безпеки. Розширення до ISO/IEC 27001 та ISO/IEC 27002 для управління конфіденційною інформацією. Вимоги та вказівки», згідно з методичними рекомендаціями щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджених наказом Адміністрації державної служби спеціального зв'язку та захисту інформації в Україні від 03.07.2023 №570; на виконання листа заступника голови Київської обласної державної адміністрації з питань цифрового розвитку, цифрових трансформацій і цифровізації (CDTO), відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 №2163-VIII, Плану реалізації Стратегії кібербезпеки України, схваленого рішенням Ради національної безпеки і оборони України від 30 грудня 2021 року, введеного в дію Указом Президента України від 01 лютого 2022 року №37/2022, Порядку реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затвердженого постановою Кабінету Міністрів України від 04 квітня 2023 року №299, підвищення кіберзахисту інформації в інформаційно-

телекомунікаційних системах Переяславської міської територіальної громади, керуючись п. 20 ч. 4 ст. 42 Закону України «Про місцеве самоврядування в Україні»

ЗОБОВ'ЯЗУЮ:

1. Затвердити Політику інформаційної безпеки структурних підрозділів виконавчого комітету та Переяславської міської ради (додаток 1).
2. Затвердити План реагування на кіберінциденти (додаток 2).
3. Установити, що Політика інформаційної безпеки Переяславської міської ради є обов'язковою до виконання посадовими особами відділів, управлінь, інших виконавчих органів міської ради, які працюють з інформаційними ресурсами.
4. Визначити відповідальним за реалізацію Політики інформаційної безпеки та за реагування на кібератаки, кіберінциденти та інформування суб'єктів забезпечення кібербезпеки Переяславської міської ради - головного спеціаліста-системного адміністратора відділу організаційно-інформаційної роботи та комп'ютерного забезпечення виконавчого комітету Переяславської міської ради Павла ПИЛИПЦЯ.
5. Загальний відділ виконавчого комітету Переяславської міської ради забезпечити доведення цього розпорядження до керівників структурних підрозділів виконавчого комітету та Переяславської міської ради.
6. Контроль за виконанням розпорядження залишаю за собою.

Міський голова **Вячеслав САУЛКО**

ВИКОНАВЧИЙ КОМІТЕТ ПЕРЕЯСЛАВСЬКОЇ МІСЬКОЇ РАДИ Ідентифікаційний код 33201806 УКРАЇНА

Тетяна КОНДРАТЕНКО
Вікторія КОВАЛЕНКО
Павло ПИЛИПЕЦЬ

Наталія ЛЕБІДЬ
Вікторія БРЕНЬ
Марія ГЛАДЧЕНКО

Додаток 1
до розпорядження міського голови
26.11. 2025 року № 278/07-04/11-25

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
Переяславської міської ради та її структурних підрозділів

1. Загальні положення

Політика інформаційної безпеки (далі – Політика) визначає загальні вимоги до інформаційної безпеки у Переяславській міській територіальній громаді (далі – МТГ), основні принципи, цілі та завдання управління інформаційною безпекою МТГ.

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

Ця Політика є офіційно прийнятою Керівництвом МТГ 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 даної Політики є:

- забезпечення захисту інформаційних ресурсів МТГ від зовнішніх і внутрішніх загроз;
- безперервність роботи всіх служб і сервісів МТГ;
- мінімізація ризиків операційної діяльності МТГ;
- створення позитивної репутації МТГ при взаємодії з третіми сторонами;
- відповідність законодавству України та вимогам контролюючих органів в області інформаційної безпеки та захисту персональних даних.

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

2. Терміни та визначення

Власник ІА – співробітник МТГ, 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 ІБ, що проводиться співробітниками МТГ, 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 МТГ, 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 МТГ, 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 Організацію. Даний процес використовує результати оцінок загроз і вразливостей для виявлення ризиків для діяльності МТГ 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 МТГ та пов'язаних з нею ресурсів.

Ризик – ймовірність впливу на діяльність МТГ (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 МТГ. Співробітники МТГ та відповідні треті сторони (які мають доступ до інформації та/або ресурсів МТГ) 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 МТГ.

Суттєвими змінами можна вважати:

- зміни в процесах діяльності МТГ;
- зміни в організаційній структурі;
- зміни в ІТ-інфраструктурі МТГ тощо.

Відповідно до сфери діяльності МТГ необхідно також враховувати наступні моменти:

- законодавство, що регулює сферу діяльності МТГ та договірні зобов'язання;
- відповідальність за порушення Політики;

- обов'язки керівництва МТГ та інших осіб щодо безпеки систем та інформації МТГ.

3.2. Розподіл обов'язків з інформаційної безпеки

Загальна відповідальність за ІБ МТГ покладається на Керівництво. Конфліктні обов'язки та сфери відповідальності повинні бути розділені, щоб зменшити можливості для несанкціонованих або ненавмисних змін чи зловживання ІА МТГ.

Формальне розподілення відповідальності Керівництвом МТГ забезпечує стратегічну прозорість та вплив на практику забезпечення ІБ.

Керівництво відповідальне за:

- визначення критичних операційних процесів для діяльності МТГ;
- прийняття рішень щодо розвитку ІБ МТГ;
- затвердження та поширення правил і вимог ІБ в МТГ;
- затвердження відповідальності за порушення правил та вимог ІБ;
- функцію перевірки та контролю виконання в МТГ 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 МТГ та третьої сторони, якому надано доступ до систем та/або даних МТГ, несе відповідальність за безпечне використання систем і даних для цілей діяльності МТГ 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 МТГ.

Обов'язок Керівництва МТГ вимагати від всіх співробітників та третіх сторін дотримання вимог ІБ МТГ, 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

Всі співробітники, які є користувачами внутрішньої мережі повинні бути ознайомлені з внутрішніми вимогами щодо роботи з інформаційними активами МТГ 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 МТГ. 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 МТГ. Для входу в зони обмеженого доступу (серверні, фінансовий відділ тощо) співробітники/третя сторона повинні мати відповідний рівень доступу. Цей рівень затверджується Керівництвом МТГ.

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

Ідентифікатори доступу мають видаватися під час адаптації співробітників в МТГ 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 МТГ 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 МТГ, 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 МТГ повинні бути визначені та задокументовані в Реєстрі ІА.

ІА МТГ можуть включати:

- інформацію про МТГ та зацікавлені треті сторони (підрядники, партнери, клієнти тощо),
- системи, послуги чи обладнання, в яких обробляється, зберігається або передається інформація про МТГ та зацікавлених третіх сторін.

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

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

3.9. Використання особистих пристроїв

МТГ 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.

МТГ 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 МТГ, 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 МТГ, 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 МТГ, 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 МТГ, 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 МТГ;
- 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 МТГ для виконання своїх службових обов'язків. Використання електронної пошти співробітниками МТГ в особистих або інших цілях, не пов’язаних з діяльністю МТГ, заборонено.

В МТГ 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 МТГ 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 МТГ, 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

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

Робочі пристрої користувачів в МТГ 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 МТГ (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 МТГ.

3.15. Встановлення безпечних оновлень

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

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.

МТГ 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 МТГ.

МТГ 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 МТГ.

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

МТГ 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 МТГ 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 МТГ.

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

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

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

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.

МТГ 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 МТГ 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 МТГ. У разі неможливості зміни систем чи сервісів, такі винятки повинні бути погоджені з Керівництвом.

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

3.20. Віддалений доступ

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

Інше використання Інтернет-ресурсів слід розглядати як порушення.

Підключення до мережі Інтернет в МТГ 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 МТГ 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 МТГ 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 МТГ.

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

3.22. Безпека комунікацій

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

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

Заборонений доступ до ресурсів МТГ за прямим посиланням.

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

В МТГ 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

МТГ 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 МТГ. Метою управління ризиками є надання Керівництву МТГ інформації, необхідної для прийняття обґрунтованих рішень щодо зміни пріоритетів діяльності для управління областями неприйнятно високого ризику.

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

МТГ повинна підтримувати План реагування на інциденти кібербезпеки (Додаток 2), який повинен спиратися на постійний оперативний моніторинг і процедури реагування на інциденти. МТГ повинна регулярно проводити навчання та підвищення обізнаності персоналу в сфері управління інцидентами.