МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«МІЖНАРОДНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ
«МИКОЛАЇВСЬКА ПОЛІТЕХНІКА»

ПОЛОЖЕННЯ ПРО КІБЕРБЕЗПЕКУ ТА ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ

(редакція 1-2025, протокол Вченої ради ВНЗ МТУ «Миколаївська політехніка» № 01/26 від 27 грудня 2025 р. затверджених наказом ректора від 27 грудня 2025 року № 164)

ЗАТВЕРДЖЕНО
Вченою радою ВНЗ «Міжнародний технологічний університет «Миколаївська політехніка»
Протокол № 02/25 від «28» лютого 2025 р.

Голова Вченої ради ВНЗ «Міжнародний технологічний університет «Миколаївська політехніка»
_____ Є. С. Полякова
«02» лютого 2025 р.

Набуває чинності згідно з наказом ректора від «28» лютого 2025 р. № 08/01

Миколаїв, 2025 р.

ЗМІСТ

РОЗДІЛ 1 ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Це Положення визначає організаційні та правові засади забезпечення кібербезпеки та захисту інформаційних ресурсів у Вищому навчальному закладі «Міжнародний технологічний університет «Миколаївська політехніка» (далі – Університет).

1.2. Положення встановлює основні вимоги щодо організації системи кібербезпеки, захисту цифрової інфраструктури, попередження кіберзагроз, реагування на кіберінциденти та забезпечення безпечного використання інформаційних ресурсів Університету.

1.3. Положення розроблено відповідно до Конституції України, Законів України «Про освіту», «Про вищу освіту», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», «Про електронні документи та електронний документообіг», «Про електронну ідентифікацію та електронні довірчі послуги», інших нормативно-правових актів України та внутрішніх нормативних документів Університету.

1.4. Дія цього Положення поширюється на всіх працівників Університету, здобувачів освіти, осіб, які виконують роботи або надають послуги для Університету, а також інших користувачів інформаційних ресурсів Університету.

1.5. Вимоги цього Положення є обов'язковими для виконання всіма особами, які мають доступ до інформаційних ресурсів, мережевого обладнання, серверів, програмного забезпечення та інших цифрових активів Університету.

1.6. Кібербезпека в Університеті є складовою системи управління та спрямована на забезпечення стабільного функціонування інформаційної інфраструктури, безперервності освітнього процесу та захисту інформаційних ресурсів від внутрішніх і зовнішніх загроз.

1.7. Об'єктами захисту в Університеті є:

- інформаційні ресурси;
- інформаційно-комунікаційні системи;
- серверне обладнання;
- комп'ютерна техніка;
- мережеве обладнання;
- програмне забезпечення;
- електронні бази даних;
- офіційні вебресурси Університету;
- хмарні сервіси;
- електронні архіви;
- цифрові документи;
- інші цифрові активи Університету.

1.8. Забезпечення кібербезпеки здійснюється на принципах:

- законності;
- безперервності захисту;
- комплексності заходів безпеки;
- своєчасного виявлення загроз;
- мінімізації ризиків;

- персональної відповідальності користувачів;
- конфіденційності інформації;
- цілісності інформаційних ресурсів;
- доступності інформаційних систем.

1.9. Університет забезпечує впровадження організаційних, технічних та профілактичних заходів, спрямованих на запобігання кіберзагрозам та несанкціонованому втручанню в роботу інформаційних систем.
1.10. Інформаційні ресурси Університету використовуються виключно для виконання освітніх, наукових, управлінських, адміністративних та інших завдань, пов'язаних із діяльністю Університету.
1.11. Не допускається використання інформаційних ресурсів Університету для діяльності, що суперечить законодавству України або може створювати загрозу інформаційній безпеці Університету.
1.12. Університет здійснює заходи щодо захисту інформаційних ресурсів від:

- несанкціонованого доступу;
- шкідливого програмного забезпечення;
- кібератак;
- втрати інформації;
- пошкодження інформації;
- блокування інформаційних систем;
- несанкціонованої модифікації даних;
- витоку інформації;
- інших кіберзагроз.

1.13. Для забезпечення належного рівня кібербезпеки Університет може використовувати спеціалізовані програмні та технічні засоби захисту інформації.
1.14. Користувачі інформаційних ресурсів зобов'язані дотримуватися вимог кібербезпеки та правил роботи з цифровими ресурсами Університету.
1.15. Кожен користувач несе персональну відповідальність за безпечне використання наданих йому засобів доступу до інформаційних ресурсів.
1.16. Університет забезпечує організацію заходів з підвищення обізнаності працівників та здобувачів освіти щодо питань кібербезпеки.
1.17. Заходи кібербезпеки реалізуються з урахуванням особливостей організації освітнього процесу, структури Університету та наявної цифрової інфраструктури.
1.18. Умови воєнного стану, постійні кіберзагрози та ризики для об'єктів критичної інформаційної інфраструктури держави вимагають посиленої уваги до забезпечення кібербезпеки та захисту інформаційних ресурсів Університету.
1.19. У разі виникнення кіберінцидентів, надзвичайних ситуацій або загроз функціонуванню інформаційних систем Університет вживає заходів щодо локалізації наслідків, відновлення працездатності інформаційних ресурсів та недопущення повторення таких випадків.
1.20. Організація системи кібербезпеки в Університеті повинна забезпечувати безперервність освітньої, наукової та управлінської діяльності незалежно від місця перебування працівників і здобувачів освіти.

1.21. Терміни та поняття, що використовуються у цьому Положенні, застосовуються у значеннях, визначених законодавством України у сфері кібербезпеки, захисту інформації та інформаційно-комунікаційних технологій.
1.22. Це Положення є базовим внутрішнім документом Університету з питань кібербезпеки та підлягає застосуванню всіма користувачами інформаційних ресурсів Вищого навчального закладу «Міжнародний технологічний університет «Миколаївська політехніка».

РОЗДІЛ 2 МЕТА ТА ОСНОВНІ ЗАВДАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

2.1. Метою забезпечення кібербезпеки у Вищому навчальному закладі «Міжнародний технологічний університет «Миколаївська політехніка» є створення безпечного цифрового середовища для здійснення освітньої, наукової, управлінської, адміністративної та іншої діяльності Університету.
2.2. Забезпечення кібербезпеки спрямоване на захист інформаційних ресурсів, цифрової інфраструктури та інформаційно-комунікаційних систем Університету від внутрішніх і зовнішніх кіберзагроз.
2.3. Кібербезпека є одним із важливих елементів системи управління Університетом та забезпечує стабільне функціонування інформаційних ресурсів і цифрових сервісів.
2.4. Основною метою кібербезпеки є забезпечення:

- конфіденційності інформації;
- цілісності інформаційних ресурсів;
- доступності інформаційних систем;
- безперервності функціонування цифрової інфраструктури;
- стійкості інформаційних ресурсів до кіберзагроз.

2.5. Система кібербезпеки Університету спрямована на попередження, виявлення та мінімізацію наслідків кіберінцидентів.
2.6. Основними завданнями забезпечення кібербезпеки є:

- захист інформаційних ресурсів Університету;
- захист інформаційно-комунікаційних систем;
- забезпечення безпечного використання цифрових сервісів;
- запобігання несанкціонованому доступу до інформації;
- попередження кіберінцидентів;
- своєчасне виявлення кіберзагроз;
- підвищення рівня кіберстійкості Університету.

2.7. Одним із ключових завдань є забезпечення належного рівня захисту цифрової інфраструктури Університету.
2.8. До цифрової інфраструктури Університету належать:

- серверне обладнання;
- локальні комп'ютерні мережі;
- мережеве обладнання;
- системи зберігання даних;
- інформаційні системи;
- вебресурси Університету;

- хмарні сервіси;
- інші цифрові ресурси.

2.9. Забезпечення кібербезпеки передбачає впровадження комплексу організаційних та технічних заходів захисту інформації.
2.10. Важливим завданням є забезпечення стійкості інформаційних ресурсів до зовнішніх впливів та кіберзагроз.
2.11. Система кібербезпеки повинна забезпечувати своєчасне виявлення спроб несанкціонованого доступу до інформаційних ресурсів.
2.12. Університет здійснює заходи щодо попередження:

- комп'ютерних вірусів;
- шкідливого програмного забезпечення;
- фішингових атак;
- спроб викрадення даних;
- атак на вебресурси;
- атак на серверну інфраструктуру;
- блокування інформаційних систем;
- інших видів кіберзагроз.

2.13. Одним із завдань кібербезпеки є забезпечення безперервності роботи інформаційних систем Університету.
2.14. Для досягнення цієї мети можуть використовуватися резервні механізми зберігання інформації та відновлення працездатності цифрової інфраструктури.
2.15. Університет забезпечує реалізацію заходів щодо мінімізації ризиків втрати інформації.
2.16. Особлива увага приділяється захисту інформаційних ресурсів, що використовуються для забезпечення освітньої діяльності, управління Університетом та взаємодії зі здобувачами освіти.
2.17. Важливим завданням є формування культури кібербезпеки серед працівників та здобувачів освіти.
2.18. Університет сприяє підвищенню рівня обізнаності користувачів щодо сучасних кіберзагроз та способів їх попередження.
2.19. Система кібербезпеки повинна забезпечувати можливість оперативного реагування на кіберінциденти та відновлення функціонування інформаційних ресурсів.
2.20. Одним із завдань є організація ефективної взаємодії між структурними підрозділами Університету під час реагування на кіберінциденти.
2.21. Університет забезпечує здійснення контролю за дотриманням вимог кібербезпеки всіма користувачами інформаційних ресурсів.
2.22. Для оцінювання ефективності заходів кібербезпеки можуть проводитися перевірки, моніторинг та аналіз стану захищеності інформаційних ресурсів.
2.23. В умовах воєнного стану забезпечення кібербезпеки є одним із пріоритетних напрямів діяльності Університету.
2.24. З огляду на зростання кількості кіберзагроз під час воєнного стану Університет вживає додаткових заходів щодо захисту інформаційних ресурсів та цифрової інфраструктури.
2.25. Особлива увага приділяється забезпеченню безперервності функціонування

інформаційних систем незалежно від місця перебування працівників та здобувачів освіти.
2.26. У разі виникнення кіберінцидентів або надзвичайних ситуацій Університет забезпечує реалізацію заходів щодо локалізації загроз, збереження інформації та відновлення працездатності інформаційних ресурсів.
2.27. Реалізація мети та завдань забезпечення кібербезпеки спрямована на створення надійного цифрового середовища, підвищення стійкості інформаційної інфраструктури та забезпечення безпечної діяльності Вищого навчального закладу «Міжнародний технологічний університет «Миколаївська політехніка».

РОЗДІЛ 3 ОРГАНІЗАЦІЯ СИСТЕМИ КІБЕРБЕЗПЕКИ УНІВЕРСИТЕТУ

3.1. Система кібербезпеки у Вищому навчальному закладі «Міжнародний технологічний університет «Миколаївська політехніка» є сукупністю організаційних, технічних, програмних та управлінських заходів, спрямованих на забезпечення захисту інформаційних ресурсів та цифрової інфраструктури Університету.
3.2. Організація системи кібербезпеки здійснюється відповідно до законодавства України, внутрішніх нормативних документів Університету та цього Положення.
3.3. Система кібербезпеки функціонує як складова системи управління Університетом та охоплює всі інформаційні ресурси, інформаційні системи та цифрові сервіси, що використовуються у діяльності Університету.
3.4. Організація кібербезпеки базується на принципах:

- комплексності заходів захисту;
- безперервності функціонування;
- своєчасного реагування на загрози;
- розмежування доступу;
- мінімізації ризиків;
- персональної відповідальності користувачів;
- постійного вдосконалення системи захисту.

3.5. Загальне керівництво діяльністю у сфері кібербезпеки здійснює ректор Університету.
3.6. Координація заходів із забезпечення кібербезпеки може покладатися на визначений структурний підрозділ, відповідальну посадову особу або робочу групу відповідно до організаційної структури Університету.
3.7. Керівники структурних підрозділів забезпечують виконання вимог кібербезпеки працівниками відповідних підрозділів.
3.8. Працівники Університету зобов'язані дотримуватися встановлених вимог щодо безпечного використання інформаційних ресурсів та цифрових сервісів.
3.9. Система кібербезпеки охоплює:

- організацію захисту інформаційних ресурсів;
- управління доступом до цифрових ресурсів;
- захист мережевої інфраструктури;
- захист серверного обладнання;
- резервування даних;
- моніторинг кіберзагроз;

- реагування на кіберінциденти;
- контроль стану кібербезпеки.

3.10. До складу цифрової інфраструктури Університету можуть входити:
- сервери;
- комп'ютерна техніка;
- локальні мережі;
- мережеве обладнання;
- системи зберігання даних;
- офіційний вебсайт Університету;
- електронні сервіси;
- хмарні ресурси;
- інші інформаційні системи.

3.11. Для забезпечення належного рівня кібербезпеки Університет може використовувати спеціалізовані програмні та технічні засоби захисту інформації.
3.12. Університет забезпечує централізоване управління інформаційними ресурсами, що використовуються в освітній, науковій та адміністративній діяльності.
3.13. Організація кібербезпеки передбачає визначення рівнів доступу до інформаційних ресурсів відповідно до посадових обов'язків користувачів.
3.14. Надання доступу до інформаційних ресурсів здійснюється за принципом необхідності виконання службових або освітніх функцій.
3.15. Рішення щодо надання, зміни або припинення доступу до інформаційних ресурсів приймаються відповідно до встановленого порядку.
3.16. Університет забезпечує облік основних інформаційних ресурсів та цифрових активів.
3.17. Під час організації системи кібербезпеки враховуються потенційні ризики для інформаційних ресурсів та цифрової інфраструктури.
3.18. Для зниження ризиків можуть застосовуватися:
- організаційні заходи захисту;
- технічні засоби захисту;
- програмні засоби контролю;
- резервне копіювання;
- контроль доступу;
- моніторинг подій безпеки.

3.19. Університет забезпечує функціонування механізмів виявлення та реєстрації подій, які можуть свідчити про виникнення кіберзагроз.
3.20. Інформація про виявлені загрози може використовуватися для аналізу ризиків та вдосконалення заходів кіберзахисту.
3.21. Система кібербезпеки повинна забезпечувати можливість оперативного реагування на кіберінциденти.
3.22. Для забезпечення стійкості цифрової інфраструктури можуть формуватися резервні механізми збереження інформації та відновлення працездатності інформаційних систем.
3.23. Університет здійснює заходи щодо забезпечення безперервності функціонування критично важливих інформаційних ресурсів.

3.24. Особлива увага приділяється захисту інформаційних ресурсів, що забезпечують управлінську діяльність Університету.
3.25. Організація системи кібербезпеки передбачає взаємодію між структурними підрозділами під час вирішення питань захисту інформаційних ресурсів.
3.26. У разі необхідності до виконання окремих заходів із кібербезпеки можуть залучатися зовнішні фахівці або спеціалізовані організації відповідно до законодавства України.
3.27. Університет сприяє підвищенню рівня цифрової грамотності та кібергігієни працівників і здобувачів освіти.
3.28. Інформування користувачів щодо актуальних кіберзагроз є складовою системи кібербезпеки Університету.
3.29. Для оцінювання ефективності системи кібербезпеки можуть проводитися внутрішні перевірки, моніторинг та аналіз стану захищеності інформаційних ресурсів.
3.30. Результати таких перевірок використовуються для вдосконалення організаційних та технічних заходів захисту.
3.31. В умовах воєнного стану система кібербезпеки функціонує з урахуванням підвищених ризиків кіберзагроз та необхідності забезпечення безперервності діяльності Університету.
3.32. Особлива увага приділяється захисту інформаційних ресурсів від кібератак, спроб несанкціонованого доступу та інших загроз, характерних для умов воєнного стану.
3.33. У разі виникнення надзвичайних ситуацій Університет забезпечує реалізацію заходів щодо локалізації наслідків кіберінцидентів та відновлення працездатності інформаційних систем.
3.34. Організація системи кібербезпеки спрямована на забезпечення надійного функціонування цифрової інфраструктури, захисту інформаційних ресурсів та створення безпечного цифрового середовища Вищого навчального закладу «Міжнародний технологічний університет «Миколаївська політехніка».

РОЗДІЛ 4 ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТА ЦИФРОВОЇ ІНФРАСТРУКТУРИ

4.1. Захист інформаційних ресурсів та цифрової інфраструктури у Вищому навчальному закладі «Міжнародний технологічний університет «Миколаївська політехніка» здійснюється з метою забезпечення стабільного функціонування інформаційних систем, збереження даних та мінімізації ризиків, пов'язаних із кіберзагрозами.
4.2. Захисту підлягають усі інформаційні ресурси та елементи цифрової інфраструктури Університету незалежно від форми їх розміщення та способу використання.
4.3. До інформаційних ресурсів Університету належать:

- електронні бази даних;
- електронні реєстри;
- цифрові архіви;
- офіційні вебресурси;

- інформаційні системи;
- програмне забезпечення;
- електронні документи;
- службова інформація;
- інші цифрові активи Університету.

4.4. До об'єктів цифрової інфраструктури належать:

- серверне обладнання;
- робочі станції користувачів;
- мережеве обладнання;
- канали передачі даних;
- системи зберігання інформації;
- системи резервного копіювання;
- хмарні сервіси;
- телекомунікаційні засоби;
- інші технічні ресурси Університету.

4.5. Університет забезпечує реалізацію комплексу організаційних та технічних заходів щодо захисту інформаційних ресурсів від зовнішніх та внутрішніх загроз.

4.6. Основними напрямами захисту є:

- попередження несанкціонованого доступу;
- захист від шкідливого програмного забезпечення;
- забезпечення цілісності інформації;
- забезпечення доступності інформаційних ресурсів;
- резервування даних;
- відновлення інформаційних систем після збоїв;
- моніторинг стану захищеності ресурсів.

4.7. Університет забезпечує використання програмних засобів захисту інформації відповідно до наявних технічних можливостей та потреб діяльності.

4.8. На комп'ютерній техніці та серверах повинні використовуватися програмні засоби, що забезпечують виявлення та запобігання шкідливому програмному впливу.

4.9. Університет здійснює контроль за актуальністю програмного забезпечення, що використовується в інформаційній інфраструктурі.

4.10. Оновлення програмного забезпечення повинно здійснюватися в установленому порядку з метою усунення відомих вразливостей та підвищення рівня захисту.

4.11. Не допускається використання програмного забезпечення, походження якого неможливо підтвердити або яке створює загрозу інформаційній безпеці Університету.

4.12. Університет забезпечує захист офіційних вебресурсів від несанкціонованого втручання, зміни інформації або порушення їх працездатності.

4.13. Для захисту вебресурсів можуть застосовуватися засоби контролю доступу, резервного копіювання та моніторингу працездатності.

4.14. Захист серверної інфраструктури передбачає:

- обмеження доступу до серверів;
- контроль облікових записів;

- резервне копіювання даних;
- ведення журналів подій;
- контроль конфігурацій;
- моніторинг працездатності обладнання.

4.15. Фізичний доступ до серверного обладнання надається лише уповноваженим особам.
4.16. Розміщення серверного обладнання повинно забезпечувати його захист від несанкціонованого доступу та негативного впливу зовнішніх факторів.
4.17. Університет забезпечує захист локальної мережевої інфраструктури від несанкціонованого підключення та втручання.
4.18. Для мережевих ресурсів можуть застосовуватися механізми ідентифікації, автентифікації та контролю доступу.
4.19. Облікові записи користувачів повинні використовуватися виключно особами, яким вони надані.
4.20. Забороняється передавати облікові дані іншим особам або використовувати облікові записи без відповідних повноважень.
4.21. Одним із ключових елементів захисту інформаційних ресурсів є резервне копіювання інформації.
4.22. Резервному копіюванню можуть підлягати:

- бази даних;
- конфігурації інформаційних систем;
- електронні документи;
- службова інформація;
- цифрові архіви;
- інші інформаційні ресурси.

4.23. Резервні копії повинні зберігатися у спосіб, який забезпечує можливість відновлення інформації у разі виникнення кіберінцидентів або технічних збоїв.
4.24. Університет забезпечує контроль цілісності інформаційних ресурсів та вживає заходів щодо недопущення їх несанкціонованої зміни.
4.25. Для захисту цифрової інфраструктури можуть використовуватися системи моніторингу та реєстрації подій безпеки.
4.26. Інформація про події безпеки може використовуватися для аналізу кіберризиків та вдосконалення заходів захисту.
4.27. Університет здійснює періодичний аналіз стану захищеності інформаційних ресурсів та цифрової інфраструктури.
4.28. За результатами аналізу можуть розроблятися додаткові заходи щодо підвищення рівня кіберзахисту.
4.29. Підрядні організації та особи, які мають доступ до інформаційних ресурсів Університету, повинні дотримуватися вимог кібербезпеки, встановлених Університетом.
4.30. Надання доступу зовнішнім користувачам до інформаційних ресурсів здійснюється лише за наявності службової необхідності та відповідного рішення уповноважених осіб.
4.31. В умовах воєнного стану захист інформаційних ресурсів та цифрової інфраструктури здійснюється з урахуванням підвищеного рівня кіберзагроз.

4.32. Особлива увага приділяється забезпеченню працездатності інформаційних систем, що використовуються для управління діяльністю Університету та забезпечення освітнього процесу.
4.33. Університет вживає заходів щодо мінімізації наслідків можливих кібератак, втрати даних або порушення функціонування інформаційних систем.
4.34. У разі виникнення надзвичайних обставин забезпечується реалізація заходів щодо відновлення інформаційних ресурсів та цифрової інфраструктури в максимально короткі строки.
4.35. Захист інформаційних ресурсів та цифрової інфраструктури є безперервним процесом і здійснюється протягом усього періоду функціонування відповідних інформаційних систем.
4.36. Реалізація заходів захисту інформаційних ресурсів та цифрової інфраструктури спрямована на забезпечення стабільної діяльності Університету, підвищення його кіберстійкості та створення безпечного цифрового середовища для всіх користувачів інформаційних ресурсів.

РОЗДІЛ 5 УПРАВЛІННЯ ДОСТУПОМ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ

5.1. Управління доступом до інформаційних ресурсів у Вищому навчальному закладі «Міжнародний технологічний університет «Миколаївська політехніка» здійснюється з метою забезпечення належного рівня кібербезпеки, захисту інформації та запобігання несанкціонованому доступу до цифрових ресурсів Університету.
5.2. Управління доступом є складовою системи кібербезпеки Університету та охоплює процедури надання, зміни, обмеження, контролю та припинення доступу до інформаційних ресурсів.
5.3. Доступ до інформаційних ресурсів надається виключно в межах службових, освітніх, наукових або інших функцій, пов'язаних із діяльністю Університету.
5.4. Надання доступу здійснюється відповідно до принципу мінімально необхідних повноважень, за яким користувач отримує лише ті права доступу, які необхідні для виконання його обов'язків.
5.5. Університет забезпечує розмежування прав доступу до інформаційних ресурсів залежно від категорії користувачів та їх функціональних повноважень.
5.6. Основними категоріями користувачів можуть бути:

- керівництво Університету;
- науково-педагогічні працівники;
- педагогічні працівники;
- працівники структурних підрозділів;
- здобувачі освіти;
- адміністратори інформаційних систем;
- зовнішні користувачі;
- інші особи відповідно до їх повноважень.

5.7. Кожному користувачу надається персональний обліковий запис для роботи з інформаційними ресурсами Університету.
5.8. Персональний обліковий запис є індивідуальним засобом доступу та не може використовуватися іншими особами.

5.9. Користувач несе персональну відповідальність за всі дії, виконані під його обліковим записом.
5.10. Надання доступу до інформаційних ресурсів здійснюється на підставі:
- службової необхідності;
- наказу або розпорядження керівництва;
- звернення керівника структурного підрозділу;
- зарахування на навчання;
- прийняття на роботу;
- інших законних підстав.

5.11. Доступ до окремих інформаційних ресурсів може надаватися після проходження відповідної процедури авторизації та ідентифікації користувача.
5.12. Для доступу до інформаційних ресурсів можуть використовуватися:
- логін та пароль;
- багатофакторна автентифікація;
- електронна ідентифікація;
- кваліфікований електронний підпис;
- інші засоби автентифікації.

5.13. Паролі користувачів повинні відповідати вимогам безпеки та не можуть передаватися іншим особам.
5.14. Користувачі зобов'язані забезпечувати конфіденційність своїх облікових даних.
5.15. У разі підозри щодо компрометації облікового запису користувач зобов'язаний негайно повідомити відповідальну особу або адміністратора інформаційної системи.
5.16. Адміністратори інформаційних систем забезпечують:
- створення облікових записів;
- зміну прав доступу;
- блокування облікових записів;
- видалення облікових записів;
- ведення обліку користувачів;
- контроль використання ресурсів.

5.17. Зміна рівня доступу здійснюється у разі:
- зміни посадових обов'язків;
- переведення до іншого структурного підрозділу;
- зміни функціональних повноважень;
- необхідності виконання додаткових завдань.

5.18. Припинення доступу до інформаційних ресурсів здійснюється у разі:
- звільнення працівника;
- завершення навчання здобувача освіти;
- припинення договірних відносин;
- втрати підстав для доступу;
- порушення вимог кібербезпеки.

5.19. Університет забезпечує ведення обліку наданих прав доступу до інформаційних ресурсів.
5.20. Інформація про надання, зміну та припинення доступу повинна фіксуватися

у відповідних облікових документах або інформаційних системах.
5.21. Доступ до критично важливих інформаційних ресурсів може надаватися лише обмеженому колу уповноважених осіб.
5.22. Для окремих категорій інформаційних ресурсів можуть встановлюватися додаткові вимоги безпеки.
5.23. Користувачам забороняється:

- використовувати чужі облікові записи;
- передавати свої облікові дані третім особам;
- обходити встановлені механізми захисту;
- здійснювати спроби несанкціонованого доступу;
- змінювати налаштування без відповідних повноважень.

5.24. Університет може здійснювати моніторинг використання інформаційних ресурсів з метою забезпечення кібербезпеки та контролю дотримання встановлених правил.
5.25. Моніторинг здійснюється виключно в межах законодавства України та внутрішніх нормативних документів Університету.
5.26. Інформація про використання інформаційних ресурсів може використовуватися для аналізу подій безпеки та реагування на кіберінциденти.
5.27. Регулярно проводиться перегляд актуальності наданих прав доступу.
5.28. За результатами перегляду можуть прийматися рішення щодо зміни, обмеження або припинення доступу до окремих ресурсів.
5.29. Керівники структурних підрозділів зобов'язані своєчасно інформувати про необхідність зміни прав доступу працівників.
5.30. Університет забезпечує впровадження механізмів контролю доступу до серверної інфраструктури, мережевих ресурсів та інформаційних систем.
5.31. В умовах воєнного стану управління доступом здійснюється з урахуванням необхідності забезпечення безперервної роботи Університету та підвищених вимог до кіберзахисту.
5.32. Особлива увага приділяється захисту від несанкціонованого віддаленого доступу та компрометації облікових записів користувачів.
5.33. У разі виявлення загроз безпеці доступ до окремих інформаційних ресурсів може бути тимчасово обмежений або припинений до усунення відповідних ризиків.
5.34. Контроль за дотриманням вимог щодо управління доступом здійснюють керівництво Університету, відповідальні особи та адміністратори інформаційних систем у межах своїх повноважень.
5.35. Порушення встановлених правил управління доступом розглядаються відповідно до законодавства України та внутрішніх нормативних документів Університету.
5.36. Управління доступом до інформаційних ресурсів є одним із ключових елементів системи кібербезпеки Університету та спрямоване на забезпечення надійного захисту цифрової інфраструктури і безпечного використання інформаційних ресурсів.

РОЗДІЛ 6 РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРЗАГРОЗИ

6.1. Реагування на кіберінциденти та кіберзагрози у Вищому навчальному закладі «Міжнародний технологічний університет «Миколаївська політехніка» здійснюється з метою своєчасного виявлення, локалізації, усунення наслідків та недопущення повторення подій, які можуть негативно вплинути на функціонування інформаційних ресурсів та цифрової інфраструктури Університету.

6.2. Університет забезпечує постійну готовність до реагування на кіберзагрози відповідно до рівня ризиків та особливостей функціонування інформаційних систем.

6.3. Реагування на кіберінциденти є складовою системи кібербезпеки та здійснюється на принципах:

- оперативності;
- безперервності;
- координації дій;
- мінімізації наслідків;
- документування подій;
- відновлення працездатності систем;
- аналізу причин виникнення інцидентів.

6.4. Під кіберінцидентом у межах цього Положення розуміється подія або сукупність подій, що можуть створювати загрозу інформаційним ресурсам, цифровій інфраструктурі або інформаційній безпеці Університету.

6.5. До кіберінцидентів можуть належати:

- несанкціонований доступ до інформаційних ресурсів;
- спроби злому облікових записів;
- зараження шкідливим програмним забезпеченням;
- фішингові атаки;
- блокування доступу до інформаційних систем;
- несанкціонована зміна інформації;
- витік інформації;
- порушення працездатності вебресурсів;
- атаки на серверну інфраструктуру;
- інші події, що створюють загрозу кібербезпеці.

6.6. Кожний користувач інформаційних ресурсів Університету зобов'язаний негайно повідомляти про виявлені ознаки кіберінциденту або кіберзагрози.

6.7. Повідомлення про кіберінцидент може подаватися:

- безпосередньому керівнику;
- відповідальній особі з питань кібербезпеки;
- адміністратору інформаційної системи;
- іншій уповноваженій особі.

6.8. Після отримання повідомлення проводиться первинна оцінка події та визначається рівень її впливу на діяльність Університету.

6.9. Під час оцінювання враховуються:

- масштаби інциденту;
- кількість уражених ресурсів;

- ризики втрати інформації;
- вплив на освітню діяльність;
- вплив на управлінські процеси;
- можливість подальшого поширення загрози.

6.10. У разі підтвердження кіберінциденту відповідальні особи організовують заходи щодо його локалізації.
6.11. Локалізація кіберінциденту може включати:
- обмеження доступу до інформаційних ресурсів;
- блокування облікових записів;
- ізоляцію уражених пристроїв;
- відключення окремих сервісів;
- обмеження мережевої взаємодії;
- інші необхідні заходи.

6.12. Заходи локалізації повинні бути спрямовані на недопущення поширення загрози на інші інформаційні ресурси Університету.
6.13. Після локалізації кіберінциденту проводиться аналіз його причин та наслідків.
6.14. Аналіз повинен передбачати:
- встановлення джерела загрози;
- визначення способу реалізації атаки;
- оцінювання обсягу завданої шкоди;
- визначення вразливостей, що були використані;
- підготовку рекомендацій щодо усунення причин інциденту.

6.15. За результатами аналізу можуть розроблятися додаткові організаційні та технічні заходи безпеки.
6.16. Усі кіберінциденти підлягають обліку та документуванню.
6.17. Інформація про кіберінциденти вноситься до журналу реєстрації кіберінцидентів та порушень інформаційної безпеки.
6.18. Документування кіберінцидентів повинно містити:
- дату та час події;
- опис інциденту;
- перелік уражених ресурсів;
- вжиті заходи реагування;
- результати розгляду;
- рекомендації щодо запобігання повторенню.

6.19. Університет забезпечує збереження інформації про кіберінциденти для подальшого аналізу та вдосконалення системи кібербезпеки.
6.20. У разі порушення працездатності інформаційних систем здійснюються заходи щодо їх відновлення.
6.21. Відновлення може включати:
- відновлення даних із резервних копій;
- відновлення роботи серверів;
- відновлення мережевих сервісів;
- перевірку цілісності інформації;
- тестування працездатності систем.

6.22. Після завершення відновлювальних робіт проводиться перевірка безпечності функціонування відповідних ресурсів.
6.23. Університет здійснює аналіз тенденцій та причин виникнення кіберінцидентів.
6.24. Результати аналізу використовуються для вдосконалення внутрішніх процедур реагування та підвищення рівня кіберстійкості.
6.25. У разі необхідності Університет може взаємодіяти з державними органами, спеціалізованими установами або іншими суб'єктами у сфері кібербезпеки відповідно до законодавства України.
6.26. Взаємодія здійснюється з метою отримання консультаційної, методичної або технічної допомоги під час реагування на кіберінциденти.
6.27. Особлива увага приділяється реагуванню на інциденти, що можуть вплинути на функціонування освітньої діяльності, офіційного вебсайту Університету, електронних сервісів та інформаційних ресурсів управлінського характеру.
6.28. Університет забезпечує готовність до реагування на кіберзагрози, що можуть виникати внаслідок використання віддаленого доступу та мережевих сервісів.
6.29. В умовах воєнного стану реагування на кіберінциденти здійснюється з урахуванням підвищеного рівня кіберзагроз та ризиків для інформаційної інфраструктури.
6.30. Особлива увага приділяється захисту критично важливих інформаційних ресурсів, що забезпечують управлінську та освітню діяльність Університету.
6.31. У разі масштабних кібератак можуть застосовуватися тимчасові додаткові заходи захисту інформаційних ресурсів та цифрової інфраструктури.
6.32. Відповідальні особи забезпечують координацію дій працівників під час ліквідації наслідків кіберінцидентів.
6.33. Користувачі інформаційних ресурсів повинні сприяти проведенню заходів реагування та виконувати законні вимоги відповідальних осіб.
6.34. Невиконання вимог щодо повідомлення про кіберінциденти або перешкоджання реагуванню на них розглядається як порушення вимог цього Положення.
6.35. Ефективне реагування на кіберінциденти є важливою умовою забезпечення безперервності діяльності Університету та захисту його інформаційних ресурсів.
6.36. Реалізація заходів реагування на кіберінциденти та кіберзагрози спрямована на мінімізацію можливих втрат, підвищення кіберстійкості та забезпечення стабільного функціонування цифрового середовища Вищого навчального закладу «Міжнародний технологічний університет «Миколаївська політехніка».

РОЗДІЛ 7 ПРАВА ТА ОБОВ'ЯЗКИ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ РЕСУРСІВ

7.1. Користувачами інформаційних ресурсів Вищого навчального закладу «Міжнародний технологічний університет «Миколаївська політехніка» є працівники Університету, здобувачі освіти, а також інші особи, яким в установленому порядку надано право доступу до інформаційних ресурсів та цифрової інфраструктури Університету.
7.2. Права та обов'язки користувачів визначаються законодавством України,

внутрішніми нормативними документами Університету та цим Положенням.
7.3. Користувачі інформаційних ресурсів мають право:
- отримувати доступ до інформаційних ресурсів відповідно до наданих повноважень;
- використовувати цифрові сервіси Університету для виконання освітніх, наукових, управлінських та службових завдань;
- отримувати технічну та консультаційну допомогу щодо використання інформаційних ресурсів;
- повідомляти про виявлені кіберзагрози, технічні несправності та порушення безпеки;
- вносити пропозиції щодо вдосконалення системи кібербезпеки.

7.4. Працівники Університету мають право використовувати інформаційні ресурси виключно в межах виконання своїх посадових обов'язків.
7.5. Здобувачі освіти мають право використовувати інформаційні ресурси Університету для забезпечення освітньої діяльності, виконання навчальних завдань та участі в інших видах діяльності, передбачених освітнім процесом.
7.6. Користувачі мають право на захист своїх облікових записів та безпечне використання інформаційних ресурсів Університету.
7.7. Університет забезпечує користувачам можливість отримання актуальної інформації щодо вимог кібербезпеки та безпечної роботи з цифровими ресурсами.
7.8. Користувачі зобов'язані дотримуватися вимог цього Положення та інших внутрішніх нормативних документів Університету у сфері кібербезпеки.
7.9. Під час використання інформаційних ресурсів користувачі зобов'язані:
- дотримуватися встановлених правил доступу;
- забезпечувати збереження облікових даних;
- використовувати інформаційні ресурси за призначенням;
- не допускати дій, що можуть створити загрозу кібербезпеці;
- виконувати вимоги відповідальних осіб з питань кібербезпеки.

7.10. Користувачі зобов'язані забезпечувати конфіденційність своїх логінів, паролів та інших засобів автентифікації.
7.11. Забороняється передавати облікові дані іншим особам або використовувати чужі облікові записи.
7.12. У разі втрати, компрометації або підозри щодо несанкціонованого використання облікового запису користувач зобов'язаний невідкладно повідомити відповідальну особу або адміністратора інформаційної системи.
7.13. Користувачі повинні використовувати лише дозволене програмне забезпечення та інформаційні ресурси, визначені Університетом.
7.14. Забороняється самостійне встановлення програмного забезпечення, яке може створити загрозу інформаційній безпеці або порушити роботу цифрової інфраструктури Університету.
7.15. Користувачі зобов'язані дотримуватися вимог щодо захисту інформації та не допускати несанкціонованого копіювання, поширення або зміни інформаційних ресурсів.
7.16. Не допускається використання інформаційних ресурсів Університету для:
- здійснення протиправної діяльності;

- розповсюдження шкідливого програмного забезпечення;
- несанкціонованого доступу до інформації;
- втручання в роботу інформаційних систем;
- порушення роботи мережевої інфраструктури;
- дій, що можуть завдати шкоди Університету.

7.17. Користувачі повинні своєчасно встановлювати рекомендовані оновлення програмного забезпечення, якщо такі оновлення передбачені правилами експлуатації відповідних ресурсів.

7.18. Працівники та здобувачі освіти зобов'язані повідомляти про:

- спроби несанкціонованого доступу;
- фішингові повідомлення;
- підозрілі електронні листи;
- виявлення шкідливого програмного забезпечення;
- порушення роботи інформаційних систем;
- інші ознаки кіберзагроз.

7.19. Повідомлення про кіберінциденти повинно здійснюватися одразу після виявлення відповідної події.

7.20. Користувачі зобов'язані сприяти проведенню заходів щодо розслідування кіберінцидентів та усунення їх наслідків.

7.21. Працівники Університету, які мають розширені права доступу до інформаційних ресурсів, несуть підвищену відповідальність за забезпечення їх належного використання.

7.22. Адміністратори інформаційних систем зобов'язані:

- забезпечувати працездатність інформаційних ресурсів;
- контролювати права доступу;
- здійснювати технічний моніторинг;
- забезпечувати виконання заходів кібербезпеки;
- реагувати на виявлені загрози.

7.23. Користувачі повинні дотримуватися вимог цифрової етики та правил безпечної поведінки в інформаційному середовищі Університету.

7.24. Не допускається використання інформаційних ресурсів для розміщення інформації, що суперечить законодавству України або завдає шкоди діловій репутації Університету.

7.25. Університет може проводити інформаційно-роз'яснювальну роботу щодо підвищення рівня кібергігієни користувачів.

7.26. Користувачі зобов'язані брати участь у заходах з підвищення обізнаності з питань кібербезпеки, якщо такі заходи організовуються Університетом.

7.27. В умовах воєнного стану користувачі повинні приділяти особливу увагу питанням кібербезпеки та дотриманню встановлених правил роботи з інформаційними ресурсами.

7.28. Під час дистанційної роботи або навчання користувачі зобов'язані забезпечувати належний рівень захисту пристроїв та каналів зв'язку, які використовуються для доступу до ресурсів Університету.

7.29. Користувачі повинні уникати використання ненадійних інформаційних ресурсів та сервісів, що можуть становити загрозу для кібербезпеки Університету.

7.30. У разі виникнення надзвичайних ситуацій користувачі повинні виконувати вказівки відповідальних осіб щодо забезпечення безпеки інформаційних ресурсів.
7.31. Невиконання вимог цього Положення розглядається як порушення правил використання інформаційних ресурсів Університету.
7.32. Особи, винні у порушенні вимог кібербезпеки, можуть бути притягнуті до відповідальності відповідно до законодавства України та внутрішніх нормативних документів Університету.
7.33. Реалізація прав та виконання обов'язків користувачів інформаційних ресурсів спрямовані на забезпечення належного рівня кібербезпеки, захисту цифрової інфраструктури та безпечного функціонування інформаційного середовища Університету.
7.34. Дотримання користувачами вимог цього Положення є необхідною умовою стабільної роботи інформаційних систем та забезпечення безперервної діяльності Вищого навчального закладу «Міжнародний технологічний університет «Миколаївська політехніка».

РОЗДІЛ 8 МОНІТОРИНГ СТАНУ КІБЕРБЕЗПЕКИ ТА ВНУТРІШНІЙ КОНТРОЛЬ

8.1. Моніторинг стану кібербезпеки та внутрішній контроль у Вищому навчальному закладі «Міжнародний технологічний університет «Миколаївська політехніка» здійснюються з метою забезпечення належного рівня захисту інформаційних ресурсів, своєчасного виявлення кіберзагроз та оцінювання ефективності заходів кібербезпеки.
8.2. Моніторинг є складовою системи кібербезпеки Університету та здійснюється на постійній основі.
8.3. Основними завданнями моніторингу є:

- виявлення потенційних кіберзагроз;
- оцінювання стану захищеності інформаційних ресурсів;
- контроль дотримання вимог кібербезпеки;
- аналіз подій інформаційної безпеки;
- попередження кіберінцидентів;
- удосконалення заходів кіберзахисту.

8.4. Внутрішній контроль здійснюється з метою перевірки дотримання працівниками та здобувачами освіти вимог цього Положення та інших внутрішніх нормативних документів Університету.
8.5. Загальний контроль за станом кібербезпеки здійснює ректор Університету.
8.6. Безпосередній моніторинг та контроль можуть здійснювати:

- проректори відповідно до розподілу повноважень;
- керівники структурних підрозділів;
- відповідальні особи з питань кібербезпеки;
- адміністратори інформаційних систем;
- комісії, створені наказом ректора;
- інші уповноважені особи.

8.7. Моніторингу підлягають:

- інформаційні ресурси Університету;

- серверна інфраструктура;
- мережеве обладнання;
- вебресурси Університету;
- цифрові сервіси;
- облікові записи користувачів;
- журнали подій інформаційних систем;
- резервні копії даних;
- інші цифрові активи.

8.8. Під час моніторингу можуть перевірятися:

- працездатність інформаційних систем;
- стан захищеності цифрової інфраструктури;
- дотримання правил доступу;
- виконання вимог кібербезпеки;
- наявність ознак несанкціонованого втручання;
- стан резервного копіювання;
- актуальність програмного забезпечення.

8.9. Моніторинг може здійснюватися із застосуванням програмних засобів контролю та аналізу подій безпеки.

8.10. Інформація, отримана під час моніторингу, використовується виключно для забезпечення кібербезпеки та захисту інформаційних ресурсів Університету.

8.11. Університет забезпечує ведення обліку подій, які можуть свідчити про виникнення кіберзагроз або порушення вимог безпеки.

8.12. До подій, що підлягають аналізу, можуть належати:

- спроби несанкціонованого доступу;
- неуспішні спроби автентифікації;
- підозріла активність користувачів;
- порушення роботи інформаційних систем;
- виявлення шкідливого програмного забезпечення;
- порушення встановлених правил використання ресурсів.

8.13. Внутрішній контроль може здійснюватися шляхом проведення:

- планових перевірок;
- позапланових перевірок;
- тематичних перевірок;
- службових розслідувань;
- аналізу журналів подій;
- оцінювання ризиків.

8.14. Планові перевірки проводяться відповідно до затверджених планів роботи Університету.

8.15. Позапланові перевірки можуть проводитися у разі виникнення кіберінцидентів, отримання інформації про можливі порушення або за рішенням керівництва Університету.

8.16. Під час проведення перевірок оцінюються:

- виконання вимог цього Положення;
- стан інформаційної інфраструктури;
- ефективність заходів кіберзахисту;

- рівень кібергігієни користувачів;
- дотримання встановлених процедур безпеки.

8.17. За результатами перевірок можуть складатися:
- акти перевірки;
- довідки;
- звіти;
- службові записки;
- рекомендації щодо усунення недоліків.

8.18. Виявлені під час перевірок недоліки підлягають усуненню у встановлені строки.
8.19. Керівники структурних підрозділів забезпечують виконання заходів щодо усунення виявлених порушень.
8.20. Результати моніторингу можуть використовуватися для оцінювання рівня кіберризиків та планування подальших заходів із кібербезпеки.
8.21. Університет здійснює періодичний аналіз ефективності реалізованих заходів захисту інформаційних ресурсів.
8.22. Аналіз результатів моніторингу спрямований на виявлення тенденцій розвитку кіберзагроз та оцінювання рівня кіберстійкості Університету.
8.23. За результатами аналізу можуть прийматися рішення щодо:
- удосконалення систем захисту;
- модернізації технічних засобів;
- посилення контролю доступу;
- впровадження додаткових заходів безпеки;
- проведення навчання користувачів.

8.24. Важливим напрямом внутрішнього контролю є перевірка готовності Університету до реагування на кіберінциденти.
8.25. Для цього можуть проводитися тестування окремих елементів цифрової інфраструктури та процедур реагування на кіберзагрози.
8.26. Університет сприяє формуванню культури кібербезпеки шляхом інформування користувачів про актуальні ризики та правила безпечної роботи.
8.27. Працівники та здобувачі освіти зобов'язані сприяти проведенню моніторингу та внутрішнього контролю в межах своїх повноважень.
8.28. У разі виявлення порушень вимог кібербезпеки відповідальні особи мають право ініціювати проведення додаткових перевірок.
8.29. В умовах воєнного стану моніторинг стану кібербезпеки здійснюється з урахуванням підвищеного рівня кіберзагроз та ризиків для інформаційної інфраструктури.
8.30. Особлива увага приділяється контролю функціонування інформаційних систем, що забезпечують освітню діяльність, управлінські процеси та електронну взаємодію Університету.
8.31. У разі виявлення ознак масштабних кібератак або інших суттєвих загроз можуть впроваджуватися додаткові заходи моніторингу та контролю.
8.32. Моніторинг та внутрішній контроль повинні забезпечувати своєчасне виявлення слабких місць у системі кібербезпеки та сприяти їх усуненню.
8.33. Результати моніторингу є підставою для прийняття управлінських рішень

щодо розвитку системи кібербезпеки Університету.
8.34. Контроль за виконанням заходів кібербезпеки здійснюється на всіх рівнях управління Університетом.
8.35. Моніторинг стану кібербезпеки та внутрішній контроль є безперервними процесами та здійснюються протягом усього періоду функціонування інформаційних ресурсів Університету.
8.36. Реалізація заходів моніторингу та внутрішнього контролю спрямована на забезпечення належного рівня кіберзахисту, підвищення кіберстійкості та безпечного функціонування цифрового середовища Вищого навчального закладу «Міжнародний технологічний університет «Миколаївська політехніка».

РОЗДІЛ 9 ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ВИМОГ КІБЕРБЕЗПЕКИ

9.1. Особи, які мають доступ до інформаційних ресурсів Вищого навчального закладу «Міжнародний технологічний університет «Миколаївська політехніка», несуть персональну відповідальність за дотримання вимог цього Положення, інших внутрішніх нормативних документів Університету та законодавства України у сфері кібербезпеки та захисту інформації.
9.2. Відповідальність за порушення вимог кібербезпеки настає незалежно від форми доступу до інформаційних ресурсів та способу використання цифрової інфраструктури Університету.
9.3. Порушенням вимог кібербезпеки вважаються дії або бездіяльність, які призвели або могли призвести до:

- порушення конфіденційності інформації;
- порушення цілісності інформаційних ресурсів;
- порушення доступності інформаційних систем;
- несанкціонованого доступу до інформації;
- виникнення кіберінцидентів;
- втрати або пошкодження даних;
- порушення функціонування цифрової інфраструктури.

9.4. До порушень вимог кібербезпеки можуть належати:

- використання чужих облікових записів;
- передача власних облікових даних іншим особам;
- розголошення інформації з обмеженим доступом;
- використання несанкціонованого програмного забезпечення;
- порушення правил роботи з інформаційними ресурсами;
- невиконання вимог щодо захисту інформації;
- недотримання встановлених процедур кібербезпеки.

9.5. Порушенням вимог кібербезпеки також вважається невиконання законних вимог посадових осіб, відповідальних за забезпечення кібербезпеки Університету.
9.6. Працівники Університету несуть відповідальність за дії, вчинені з використанням наданих їм облікових записів та засобів доступу до інформаційних ресурсів.
9.7. Користувачі інформаційних ресурсів зобов'язані забезпечувати належне зберігання засобів автентифікації та не допускати їх використання сторонніми

особами.
9.8. Невиконання вимог щодо захисту логінів, паролів та інших засобів доступу може розглядатися як порушення вимог кібербезпеки.
9.9. Працівники, які здійснюють адміністрування інформаційних систем, несуть відповідальність за належне виконання своїх функціональних обов'язків у межах наданих повноважень.
9.10. Керівники структурних підрозділів несуть відповідальність за організацію виконання вимог кібербезпеки у відповідних підрозділах.
9.11. У разі виявлення порушень вимог кібербезпеки можуть проводитися службові перевірки або службові розслідування.
9.12. Метою службового розгляду є:

- встановлення обставин події;
- визначення причин виникнення порушення;
- встановлення кола відповідальних осіб;
- оцінювання наслідків порушення;
- визначення заходів щодо усунення наслідків.

9.13. Під час проведення службового розгляду можуть використовуватися:

- матеріали моніторингу;
- журнали подій інформаційних систем;
- службові пояснення;
- результати перевірок;
- інші документи та відомості.

9.14. Особи, стосовно яких проводиться службове розслідування, мають право на надання письмових пояснень щодо обставин порушення.
9.15. За результатами службового розгляду можуть прийматися рішення щодо усунення виявлених порушень та запобігання їх повторенню.
9.16. Залежно від характеру порушення та його наслідків до винних осіб можуть застосовуватися заходи впливу відповідно до законодавства України та внутрішніх нормативних документів Університету.
9.17. Порушення вимог кібербезпеки може бути підставою для:

- обмеження доступу до інформаційних ресурсів;
- тимчасового блокування облікових записів;
- перегляду наданих повноважень;
- проведення додаткового навчання з питань кібербезпеки;
- застосування інших заходів відповідно до законодавства України.

9.18. У разі виявлення фактів, що містять ознаки правопорушень, інформація може бути передана до відповідних органів державної влади у порядку, встановленому законодавством України.
9.19. Особи, винні у завданні шкоди інформаційним ресурсам або цифровій інфраструктурі Університету, можуть нести відповідальність відповідно до законодавства України.
9.20. Відповідальність настає незалежно від того, чи було порушення вчинено умисно або внаслідок недбалості.
9.21. Невиявлення порушення на момент його вчинення не звільняє винну особу від відповідальності після встановлення відповідних обставин.

9.22. Університет забезпечує документування фактів порушень вимог кібербезпеки та зберігання відповідних матеріалів.
9.23. Інформація про порушення може використовуватися для аналізу ризиків та вдосконалення системи кібербезпеки.
9.24. Особлива увага приділяється порушенням, які можуть впливати на:

- стабільність функціонування інформаційних систем;
- діяльність структурних підрозділів;
- організацію освітнього процесу;
- збереження інформаційних ресурсів;
- функціонування цифрової інфраструктури.

9.25. Працівники та здобувачі освіти зобов'язані сприяти встановленню обставин кіберінцидентів та інших порушень вимог кібербезпеки.
9.26. Приховування фактів порушення вимог кібербезпеки або ненадання інформації про відомі кіберзагрози розглядається як невиконання вимог цього Положення.
9.27. В умовах воєнного стану вимоги щодо кібербезпеки підлягають неухильному виконанню всіма користувачами інформаційних ресурсів Університету.
9.28. Зважаючи на підвищений рівень кіберзагроз, особи, які мають доступ до інформаційних ресурсів Університету, повинні проявляти особливу обачність та відповідальність під час роботи з цифровими ресурсами.
9.29. У разі виникнення кіберінцидентів користувачі зобов'язані діяти відповідно до встановлених процедур реагування та виконувати вказівки відповідальних осіб.
9.30. Невиконання вимог щодо реагування на кіберінциденти може розглядатися як порушення вимог кібербезпеки.
9.31. Університет забезпечує справедливий та об'єктивний розгляд усіх випадків порушення вимог кібербезпеки.
9.32. Під час визначення відповідальності враховуються характер порушення, його наслідки, ступінь вини та обставини вчинення відповідних дій.
9.33. Результати розгляду порушень можуть використовуватися для вдосконалення внутрішніх процедур забезпечення кібербезпеки.
9.34. Система відповідальності за порушення вимог кібербезпеки є одним із механізмів забезпечення належного рівня захисту інформаційних ресурсів Університету.
9.35. Дотримання вимог цього Положення є обов'язком кожного користувача інформаційних ресурсів та важливою умовою безпечного функціонування цифрового середовища Університету.
9.36. Реалізація положень цього розділу спрямована на формування відповідального ставлення до питань кібербезпеки, підвищення рівня кіберкультури та забезпечення належного захисту інформаційних ресурсів Вищого навчального закладу «Міжнародний технологічний університет «Миколаївська політехніка».

РОЗДІЛ 10 ПРИКІНЦЕВІ ПОЛОЖЕННЯ

10.1. Це Положення є внутрішнім нормативним документом Вищого навчального закладу «Міжнародний технологічний університет «Миколаївська політехніка» та визначає загальні вимоги щодо забезпечення кібербезпеки і захисту інформаційних ресурсів Університету.

10.2. Вимоги цього Положення є обов'язковими для виконання всіма працівниками, здобувачами освіти та іншими особами, які мають доступ до інформаційних ресурсів, цифрової інфраструктури та електронних сервісів Університету.

10.3. Кібербезпека є невід'ємною складовою системи управління Університетом та одним із пріоритетних напрямів забезпечення безперервності його діяльності.

10.4. Організація роботи у сфері кібербезпеки здійснюється на засадах законності, відповідальності, комплексності захисту, безперервності контролю та постійного вдосконалення заходів кіберзахисту.

10.5. Університет забезпечує створення та підтримання належного рівня захисту інформаційних ресурсів відповідно до вимог законодавства України та внутрішніх нормативних документів.

10.6. Функціонування системи кібербезпеки передбачає постійне вдосконалення організаційних, технічних та профілактичних заходів захисту інформації.

10.7. Розвиток цифрової інфраструктури Університету здійснюється з урахуванням необхідності забезпечення належного рівня кібербезпеки та захисту інформаційних ресурсів.

10.8. Університет сприяє впровадженню сучасних підходів до кіберзахисту та використанню новітніх технологій у сфері інформаційної безпеки.

10.9. Керівництво Університету забезпечує необхідні організаційні умови для реалізації заходів кібербезпеки та контролю за їх виконанням.

10.10. Керівники структурних підрозділів забезпечують виконання вимог цього Положення працівниками відповідних підрозділів.

10.11. Працівники та здобувачі освіти зобов'язані дотримуватися встановлених правил кібербезпеки та сприяти підтриманню належного рівня захищеності інформаційних ресурсів.

10.12. Університет забезпечує проведення інформаційно-роз'яснювальної роботи та заходів із підвищення рівня обізнаності користувачів щодо актуальних кіберзагроз.

10.13. З метою підвищення рівня кіберстійкості можуть проводитися навчання, консультації, внутрішні перевірки та інші профілактичні заходи.

10.14. Періодичний перегляд стану кібербезпеки здійснюється для своєчасного виявлення ризиків та вдосконалення системи захисту інформаційних ресурсів.

10.15. Університет забезпечує аналіз результатів моніторингу, перевірок та кіберінцидентів для подальшого вдосконалення внутрішньої системи кібербезпеки.

10.16. Результати внутрішнього контролю можуть бути підставою для прийняття управлінських рішень щодо модернізації цифрової інфраструктури та впровадження додаткових заходів захисту.

10.17. У разі внесення змін до законодавства України положення цього документа

застосовуються в частині, що не суперечить чинним нормативно-правовим актам.
10.18. Усі питання, не врегульовані цим Положенням, вирішуються відповідно до законодавства України, Статуту Університету та інших внутрішніх нормативних документів.
10.19. Зміни та доповнення до цього Положення вносяться за рішенням Вченої ради Університету та вводяться в дію наказом ректора.
10.20. Ініціаторами внесення змін можуть бути ректор, проректори, керівники структурних підрозділів, постійні комісії, робочі групи та інші уповноважені особи.
10.21. Перегляд Положення здійснюється у разі:

- зміни законодавства України;
- зміни організаційної структури Університету;
- модернізації цифрової інфраструктури;
- виникнення нових кіберзагроз;
- необхідності вдосконалення системи кібербезпеки.

10.22. Університет забезпечує ознайомлення працівників із вимогами цього Положення в установленому порядку.
10.23. Це Положення підлягає оприлюдненню на офіційному вебсайті Університету або в іншому визначеному порядку.
10.24. Контроль за виконанням цього Положення здійснюється ректором Університету, проректорами, керівниками структурних підрозділів та іншими уповноваженими особами відповідно до їх компетенції.
10.25. В умовах воєнного стану забезпечення кібербезпеки є одним із пріоритетних напрямів діяльності Університету.
10.26. Університет вживає додаткових заходів для захисту інформаційних ресурсів від підвищених кіберризиків, характерних для умов воєнного стану.
10.27. Особлива увага приділяється забезпеченню безперервності функціонування цифрової інфраструктури, збереженню інформаційних ресурсів та підтриманню працездатності інформаційних систем.
10.28. У разі виникнення надзвичайних ситуацій або масштабних кібератак Університет забезпечує реалізацію заходів щодо відновлення функціонування інформаційних ресурсів та мінімізації негативних наслідків.
10.29. Реалізація цього Положення спрямована на створення безпечного цифрового середовища для здійснення освітньої, наукової, управлінської та адміністративної діяльності Університету.
10.30. Положення набирає чинності з дня його затвердження Вченою радою Вищого навчального закладу «Міжнародний технологічний університет «Миколаївська політехніка» та введення в дію наказом ректора.
10.31. Визнання окремих положень цього документа такими, що втратили чинність, не впливає на чинність інших його положень.
10.32. Реалізація вимог цього Положення є важливою умовою забезпечення кіберстійкості, надійного функціонування цифрової інфраструктури та ефективного розвитку Вищого навчального закладу «Міжнародний технологічний університет «Миколаївська політехніка».

ДОДАТОК 1

ФОРМА ПОВІДОМЛЕННЯ ПРО КІБЕРІНЦИДЕНТ
ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«МІЖНАРОДНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ «МИКОЛАЇВСЬКА ПОЛІТЕХНІКА»

ПОВІДОМЛЕННЯ
ПРО КІБЕРІНЦИДЕНТ

Дата подання повідомлення: «**» _____ *20*** року
Час подання повідомлення: _____

1. ВІДОМОСТІ ПРО ОСОБУ, ЯКА ПОВІДОМЛЯЄ

Прізвище, ім'я, по батькові

Посада / статус користувача

Структурний підрозділ

Контактний телефон

Електронна адреса

2. ВІДОМОСТІ ПРО КІБЕРІНЦИДЕНТ

Дата виявлення події

Час виявлення події

Місце виявлення (система, сервіс, ресурс)

Тип кіберінциденту
☐ Несанкціонований доступ
☐ Підозра на компрометацію облікового запису
☐ Фішингова атака
☐ Шкідливе програмне забезпечення
☐ Блокування доступу до ресурсу
☐ Пошкодження або зміна інформації
☐ Втрата інформації
☐ Порушення роботи вебресурсу
☐ Порушення роботи серверного обладнання
☐ Інше

3. ОПИС ПОДІЇ

Детальний опис кіберінциденту

4. ІНФОРМАЦІЙНІ РЕСУРСИ, ЯКІ МОЖУТЬ БУТИ УРАЖЕНІ

☐ Комп'ютер користувача
☐ Сервер
☐ Вебсайт Університету
☐ Локальна мережа
☐ Електронна пошта
☐ База даних
☐ Хмарний сервіс
☐ Інший ресурс

5. ПОПЕРЕДНІ НАСЛІДКИ ПОДІЇ

☐ Втрата доступу до інформації
☐ Пошкодження інформації
☐ Втрата інформації
☐ Зупинка роботи сервісу
☐ Підозра на витік інформації
☐ Інше

6. ВЖИТІ ПЕРВИННІ ЗАХОДИ

☐ Повідомлено керівника підрозділу
☐ Повідомлено адміністратора системи
☐ Змінено пароль
☐ Відключено пристрій від мережі
☐ Припинено роботу з ресурсом
☐ Інше

7. ДОДАТКОВА ІНФОРМАЦІЯ

8. ДОДАТКИ ДО ПОВІДОМЛЕННЯ

□ Скріншоти
□ Журнали подій
□ Електронні листи
□ Файли журналів
□ Інші матеріали

9. ПІДПИС ОСОБИ, ЯКА ПОДАЛА ПОВІДОМЛЕННЯ
Підпис _____
Прізвище та ініціали

Дата _____

ВІДМІТКА ПРО РЕЄСТРАЦІЮ
Реєстраційний номер повідомлення

Дата реєстрації

Відповідальна особа

Підпис

РЕЗУЛЬТАТИ РОЗГЛЯДУ
Дата розгляду

Відповідальна особа

Прийняте рішення
□ Провести перевірку
□ Зареєструвати кіберінцидент
□ Провести службове розслідування
□ Вжити заходів реагування
□ Інше

Примітки

Підпис відповідальної особи

Дата

Примітка. Повідомлення про кіберінцидент подається невідкладно після

виявлення ознак порушення кібербезпеки або загрози інформаційним ресурсам Університету та є підставою для проведення аналізу, реєстрації події та вжиття заходів реагування відповідно до Положення про кібербезпеку та захист інформаційних ресурсів.

ДОДАТОК 2

ЖУРНАЛ РЕЄСТРАЦІЇ КІБЕРІНЦИДЕНТІВ ТА ПОРУШЕНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД «МІЖНАРОДНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ «МИКОЛАЇВСЬКА ПОЛІТЕХНІКА»

ЖУРНАЛ

реєстрації кіберінцидентів та порушень інформаційної безпеки

Почато: «» ___________________ *20* року

Закінчено: «» ___________________ *20* року

Відповідальний за ведення журналу:

Посада:

ОБЛІК КІБЕРІНЦИДЕНТІВ ТА ПОРУШЕНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

№ з/п	Реєстраційний номер	Дата та час виявлення	Інформаційний ресурс	Вид кіберінциденту	Короткий опис події	Відповідальна особа	Рівень впливу	Вжиті заходи	Статус розгляду
							Низький / Середній / Високий		Відкрито / Закрито
							Низький / Середній / Високий		Відкрито / Закрито
							Низький / Середній / Високий		Відкрито / Закрито
							Низький / Середній / Високий		Відкрито / Закрито
							Низький / Середній / Високий		Відкрито / Закрито
							Низький / Середній / Високий		Відкрито / Закрито
							Низький / Середній / Високий		Відкрито / Закрито
							Низький / Середній / Високий		Відкрито / Закрито
							Низький / Середній / Високий		Відкрито / Закрито
							Низький / Середній / Високий		Відкрито / Закрито

КЛАСИФІКАЦІЯ КІБЕРІНЦИДЕНТІВ

Під час ведення журналу можуть використовуватися такі категорії подій:

Код	Вид події
KI-01	Несанкціонований доступ до інформаційних ресурсів
KI-02	Компрометація облікового запису
KI-03	Виявлення шкідливого програмного забезпечення
KI-04	Фішингова атака

Код Вид події
КІ-05 Блокування роботи інформаційної системи
КІ-06 Витік інформації
КІ-07 Пошкодження або втрата інформації
КІ-08 Порушення роботи вебресурсів
КІ-09 Порушення роботи серверного обладнання
КІ-10 Порушення політики кібербезпеки
КІ-11 Несанкціоноване використання цифрових ресурсів
КІ-12 Інші події інформаційної безпеки

ОБЛІК РЕЗУЛЬТАТІВ РОЗГЛЯДУ

№ запису Дата завершення розгляду Результат розгляду Відповідальна особа

ВІДОМОСТІ ПРО УСУНЕННЯ НАСЛІДКІВ

№ запису Вжиті заходи Дата виконання Відмітка про виконання

ПРИМІТКИ

ВІДПОВІДАЛЬНА ОСОБА ЗА ВЕДЕННЯ ЖУРНАЛУ

Посада

Прізвище, ім'я, по батькові

Підпис

Дата

Примітка. Журнал реєстрації кіберінцидентів та порушень інформаційної безпеки призначений для документування випадків порушення кібербезпеки, аналізу тенденцій виникнення кіберзагроз, контролю виконання заходів реагування та вдосконалення системи кібербезпеки ВНЗ МТУ «Миколаївська політехніка». Ведення журналу може здійснюватися в електронній або паперовій формі відповідно до внутрішніх нормативних документів Університету.

ДОДАТОК 3

АКТ ПЕРЕВІРКИ СТАНУ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ
ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«МІЖНАРОДНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ «МИКОЛАЇВСЬКА ПОЛІТЕХНІКА»

АКТ № _____
перевірки стану кібербезпеки та захисту інформаційних ресурсів

м. Миколаїв
«» **_____** ***20*** року
На підставі _____

Комісія у складі:
Голова комісії _____
Члени комісії:

провела перевірку стану кібербезпеки та захисту інформаційних ресурсів у

(найменування структурного підрозділу)
за період з «» **_____** ***20*** року по «» **_____** ***20*** року.

1. ЗАГАЛЬНІ ВІДОМОСТІ

Керівник структурного підрозділу

Відповідальна особа за інформаційну безпеку

Кількість працівників підрозділу

Кількість користувачів інформаційних ресурсів

Дата проведення перевірки

2. РЕЗУЛЬТАТИ ПЕРЕВІРКИ

№ з/п	Показник перевірки	Так	Ні	Примітка
1	Наявний контроль доступу до інформаційних ресурсів	☐	☐	
2	Використовуються персональні облікові записи	☐	☐	
3	Забезпечено захист паролів користувачів	☐	☐	
4	Використовується актуальне програмне забезпечення	☐	☐	
5	Встановлюються оновлення безпеки	☐	☐	

№ з/п	Показник перевірки	Так	Ні	Примітка
6	Використовуються антивірусні засоби захисту	☐	☐	
7	Виконується резервне копіювання інформації	☐	☐	
8	Забезпечено захист серверного обладнання	☐	☐	
9	Контролюється доступ до мережевих ресурсів	☐	☐	
10	Ведеться облік кіберінцидентів	☐	☐	
11	Наявний журнал подій безпеки	☐	☐	
12	Працівники ознайомлені з вимогами кібербезпеки	☐	☐	
13	Здійснюється реагування на кіберінциденти	☐	☐	
14	Захищено офіційні вебресурси	☐	☐	
15	Забезпечено захист електронної пошти	☐	☐	
16	Використовуються безпечні канали передачі даних	☐	☐	
17	Проводиться моніторинг інформаційних систем	☐	☐	
18	Відсутні факти несанкціонованого доступу	☐	☐	
19	Дотримуються вимоги внутрішніх документів з кібербезпеки	☐	☐	
20	Забезпечено безперервність функціонування цифрових сервісів	☐	☐	

3. ВИЯВЛЕНІ КІБЕРРИЗИКИ ТА НЕДОЛІКИ

№ з/п	Опис виявленого ризику або недоліку	Рівень ризику (низький/середній/високий)
1		
2		
3		
4		
5		

4. ВІДОМОСТІ ПРО КІБЕРІНЦИДЕНТИ

№ з/п	Дата події	Вид кіберінциденту	Наслідки	Статус усунення
1				
2				
3				
4				
5				

5. ОЦІНКА СТАНУ КІБЕРБЕЗПЕКИ

За результатами перевірки стан кібербезпеки оцінюється як:

☐ Високий

☐ Достатній

☐ Задовільний

□ Незадовільний

6. РЕКОМЕНДАЦІЇ КОМІСІЇ

1.

2.

3.

4.

5.

7. ПЛАН УСУНЕННЯ ВИЯВЛЕНИХ НЕДОЛІКІВ

№ з/п	Захід	Відповідальний	Строк виконання
1			
2			
3			
4			
5			

8. ВИСНОВОК КОМІСІЇ

Комісією встановлено, що стан кібербезпеки та захисту інформаційних ресурсів структурного підрозділу:

□ відповідає вимогам законодавства України та внутрішніх нормативних документів Університету;

□ в цілому відповідає встановленим вимогам та потребує окремих удосконалень;

□ потребує реалізації додаткових організаційних та технічних заходів;

□ не відповідає встановленим вимогам і потребує невідкладного усунення недоліків.

9. ОСОБЛИВІ ВІДМІТКИ

9.1. Перевірка проведена відповідно до Положення про кібербезпеку та захист інформаційних ресурсів ВНЗ МТУ «Миколаївська політехніка».

9.2. Під час перевірки оцінювалися організаційні, технічні та процедурні заходи забезпечення кібербезпеки.

9.3. Особливу увагу приділено захисту інформаційних ресурсів, серверної інфраструктури, цифрових сервісів та електронних комунікацій.

9.4. В умовах воєнного стану додатково перевірялися заходи забезпечення безперервності функціонування цифрової інфраструктури та готовність до реагування на кіберзагрози.

ПІДПИСИ ЧЛЕНІВ КОМІСІЇ

Голова комісії
_____ /_____/
Член комісії
_____ /_____/
Член комісії
_____ /_____/
Член комісії
_____ /_____/
Член комісії
_____ /_____/

З актом ознайомлений:
Керівник структурного підрозділу
_____ /_____/
«» _____ ***20*** року

Примітка. Акт перевірки стану кібербезпеки та захисту інформаційних ресурсів використовується для проведення внутрішнього контролю, оцінювання рівня кіберстійкості, виявлення ризиків та планування заходів із вдосконалення системи кібербезпеки ВНЗ МТУ «Миколаївська політехніка».