МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ
«ОДЕСЬКОГО НАЦІОНАЛЬНОГО ТЕХНОЛОГІЧНОГО УНІВЕРСИТЕТУ»

ЗАТВЕРДЖЕНО
педагогічною радою
ВСП «Одеського технічного
фахового коледжу ОНТУ»
26.06.2026 р. протокол № 7
Голова Педагогічної ради,
В.о. директора ВСП «ОТФК ОНТУ»

_____ Лілія ІВАНОВА
26.06.2026р.

ПОЛОЖЕННЯ ПРО КІБЕРБЕЗПЕКУ У ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Введено в дію з «01» вересня 2026р.
наказом в.о. директора
ВСП «ОТФК ОНТУ»
№ 126-М-01-ОД
від 02.07.2026 р.

Одеса – 2026 р.

ЗМІСТ

ЗАТВЕРДЖЕНО
педагогічною радою
ВСП «Одеського технічного
фахового коледжу ОНТУ»
26.06.2026р. протокол № 7
Введено в дію з «01» вересня 2026р.
наказом в.о. директора
ВСП «ОТФК ОНТУ»
від 02.07.2026р. № 126-М-01-ОД

В.о. директора ВСП «ОТФК ОНТУ»

_____ Лілія ІВАНОВА

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Це Положення визначає єдині організаційні та правові засади забезпечення технічного захисту інформації та кібербезпеки у Відокремленому структурному підрозділі «Одеський технічний фаховий коледж Одеського національного технологічного університету» (далі – Коледж), встановлює порядок організації системи технічного захисту інформації, реалізації базових заходів кібербезпеки, розподілу повноважень між посадовими особами, організації контролю та реагування на кіберінциденти.

1.2. Положення розроблено відповідно до: Конституції України; Законів України: «Про освіту»; «Про фахову передвищу освіту»; «Про інформацію»; «Про захист інформації в інформаційно-комунікаційних системах»; «Про основні засади забезпечення кібербезпеки України»; «Про захист персональних даних»; «Про електронні довірчі послуги»; «Про доступ до публічної інформації»; Указу Президента України від 27.09.1999 р. № 1229/99 «Про Положення про технічний захист інформації в Україні»; Постанови Кабінету Міністрів України від 29.03.2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах»; Постанови Кабінету Міністрів України від 18.06.2025 р. № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем»; наказів Адміністрації Державної служби спеціального зв'язку та захисту інформації України – від 03.07.2023 р. № 570, від 30.01.2025 р. № 54, від 30.06.2025 р. № 409, від 02.07.2025 р. № 419; Положення про ВСП «Одеський технічний фаховий коледж ОНТУ»; Положення «Про організацію освітнього процесу у ВСП «ОТФК ОНТУ»;

інших нормативно-правових актів України у сфері освіти, технічного захисту інформації, кібербезпеки, захисту персональних даних та електронних комунікацій.

1.3. Дія цього Положення поширюється на всіх працівників Коледжу незалежно від займаної посади, педагогічних працівників, адміністрацію, працівників структурних підрозділів, осіб, відповідальних за технічний захист інформації та кібербезпеку, адміністраторів інформаційних систем, а також здобувачів освіти у випадках використання ними інформаційних ресурсів Коледжу.

1.4. Вимоги цього Положення є обов'язковими під час:

- використання інформаційних ресурсів Коледжу;
- використання інформаційно-комунікаційних систем;
- роботи із персональними даними;
- роботи зі службовою інформацією;
- використання корпоративних електронних сервісів;
- використання засобів електронної ідентифікації;
- використання кваліфікованих електронних підписів;
- використання змінних носіїв інформації;
- використання локальної комп'ютерної мережі та мережі Інтернет.

1.5. Метою цього Положення є:

- забезпечення належного рівня технічного захисту інформації;
- забезпечення кібербезпеки інформаційних ресурсів Коледжу;
- захист персональних даних працівників та здобувачів освіти;
- забезпечення безперервності функціонування інформаційних сервісів;
- мінімізація ризиків виникнення кіберінцидентів;
- забезпечення виконання вимог чинного законодавства України.

1.6. Основними завданнями системи технічного захисту інформації та кібербезпеки є:

- організація технічного захисту інформації;
- запобігання несанкціонованому доступу;
- забезпечення цілісності та доступності інформації;
- забезпечення конфіденційності інформації;
- організація резервного копіювання;
- моніторинг стану кібербезпеки;
- реагування на кіберінциденти;
- організація навчання працівників та впровадження заходів кібергігієни;
- забезпечення виконання вимог нормативно-правових актів України.

1.7. У Коледжі технічний захист інформації та кібербезпека організовуються на основі таких принципів законності; безперервності; достатності заходів захисту; ризик-орієнтованого підходу; комплексності; відповідальності кожного користувача; мінімально необхідного доступу; персональної відповідальності посадових осіб; пропорційності заходів захисту характеру інформації; постійного удосконалення системи захисту.

1.8. Об'єктами технічного захисту інформації у Коледжі є інформація, інформаційні ресурси, інформаційно-комунікаційні системи, програмне забезпечення, технічні засоби, мережеве обладнання, електронні комунікації, персональні дані, службова інформація та інші інформаційні активи, що використовуються у діяльності Коледжу.

1.9. У Коледжі підлягає захисту, зокрема:

- інформація з обмеженим доступом;
- персональні дані працівників та здобувачів освіти;
- службова інформація;
- інформація державних інформаційних ресурсів, доступ до яких здійснюється через інформаційні системи;
- електронні документи;
- інформація, що використовується в ЄДЕБО;
- інформація бухгалтерського, кадрового, навчального та організаційного характеру;
- облікові записи користувачів;
- засоби автентифікації;
- криптографічні ключі;
- резервні копії інформації.

1.10. Організація технічного захисту інформації та кібербезпеки у Коледжі здійснюється керівником Коледжу, відповідальною особою за технічний захист інформації та кібербезпеку, керівниками структурних підрозділів та іншими працівниками в межах їхніх повноважень відповідно до законодавства України, цього Положення та інших локальних нормативних актів Коледжу.

1.11. Технічний захист інформації та кібербезпека у Коледжі забезпечуються шляхом реалізації організаційних, технічних, програмних, криптографічних, фізичних та інших заходів захисту, передбачених законодавством України та цим Положенням.

1.12. У цьому Положенні терміни «технічний захист інформації», «кібербезпека», «кіберзахист», «кіберінцидент», «інформаційно-комунікаційна система», «персональні дані», «автентифікація», «авторизація», «інформаційний ресурс», «користувач», «обліковий запис», «електронна

комунікаційна система», «резервне копіювання», «інформаційний актив» застосовуються у значеннях, визначених законами України та іншими нормативно-правовими актами у сфері технічного захисту інформації, кібербезпеки та захисту інформації.

2. ОРГАНІЗАЦІЯ СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКИ

2.1. Організація технічного захисту інформації та забезпечення кібербезпеки у Коледжі є складовою системи управління Коледжем і здійснюється з метою належного виконання вимог законодавства України щодо захисту інформації, яка обробляється під час провадження освітньої, управлінської, кадрової, фінансово-господарської, інформаційної та іншої діяльності Коледжу.

2.2. Система технічного захисту інформації та кібербезпеки Коледжу являє собою сукупність організаційних, правових, технічних, програмних, фізичних та інших заходів, локальних нормативних актів, процедур, технічних і програмних засобів, а також діяльності посадових осіб, працівників та інших користувачів інформаційних ресурсів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, запобігання кіберінцидентам, виявлення, локалізацію та усунення їх наслідків і відновлення належного функціонування інформаційних ресурсів та технічних засобів Коледжу.

2.3. Організація технічного захисту інформації та кібербезпеки здійснюється з урахуванням:

- правового режиму інформації, що обробляється;
- призначення та умов використання інформаційних ресурсів, інформаційно-комунікаційних систем, електронних комунікаційних систем, програмного забезпечення, комп’ютерної техніки та інших технічних засобів;
- вимог власників, розпорядників та адміністраторів зовнішніх інформаційних систем і сервісів, якими користується Коледж;
- актуальних кіберзагроз, виявлених вразливостей, результатів перевірок, оцінювання ризиків та аналізу кіберінцидентів;
- організаційної структури Коледжу, наявних кадрових, технічних та фінансових ресурсів;
- необхідності забезпечення безперервності основних процесів діяльності Коледжу та можливості відновлення інформації і працездатності технічних засобів після кіберінцидентів, технічних відмов тощо.

2.4. Загальне керівництво організацією технічного захисту інформації та кібербезпеки у Коледжі здійснює керівник Коледжу. Виконання спеціалізованих організаційних і технічних завдань у сфері технічного захисту

інформації та кібербезпеки покладається на відповідальну особу за технічний захист інформації та кібербезпеку (далі – відповідальна особа), призначену наказом керівника Коледжу з числа штатних працівників.

2.5. Функції з організації технічного захисту інформації та кібербезпеки виконуються відповідальною особою у взаємодії з керівником Коледжу, заступниками директора за напрямами, керівниками структурних підрозділів, адміністраторами інформаційних систем, працівниками, які використовують інформаційні ресурси та технічні засоби Коледжу, а також іншими особами в межах покладених на них повноважень.

2.6. До суб'єктів організації та забезпечення технічного захисту інформації та кібербезпеки у Коледжі належать:

- керівник (директор, в.о.директора) Коледжу;
- відповідальна особа;
- заступники директора в межах визначених функціональних повноважень;
- керівники структурних підрозділів;
- адміністратори інформаційних систем, електронних сервісів, корпоративних облікових записів та інших інформаційних ресурсів;
- працівники, яким надано доступ до інформаційних ресурсів, інформаційних систем, комп'ютерної техніки, електронних комунікацій та інших технічних засобів;
- здобувачі освіти в частині використання корпоративних інформаційних ресурсів, електронних освітніх сервісів та технічних засобів Коледжу;
- інші фізичні та юридичні особи, яким у встановленому порядку надано доступ до інформаційних ресурсів або технічної інфраструктури Коледжу.

2.7. Керівник Коледжу в межах своїх повноважень:

- забезпечує організацію виконання вимог законодавства України у сфері технічного захисту інформації, захисту інформації в системах, кібербезпеки та захисту персональних даних;
- визначає організаційні засади забезпечення технічного захисту інформації та кібербезпеки у Коледжі;
- призначає наказом відповідальну особу та визначає її повноваження;
- затверджує це Положення, інші локальні нормативні акти, процедури, плани заходів та організаційно-розпорядчі документи з питань технічного захисту інформації та кібербезпеки;
- забезпечує в межах наявних повноважень і фінансових ресурсів створення організаційних, кадрових та матеріально-технічних умов, необхідних для реалізації заходів із захисту інформації;

- приймає рішення щодо впровадження заходів захисту інформації, усунення виявлених недоліків, зниження неприйнятних ризиків та ліквідації наслідків кіберінцидентів;
- забезпечує визначення працівників, яким надається доступ до інформації, інформаційних систем та технічних засобів відповідно до їх посадових обов'язків;
- у разі необхідності створює комісії та робочі групи для розгляду питань, пов'язаних із захистом інформації, оцінюванням стану захищеності, розслідуванням обставин кіберінцидентів, втратою інформації, технічних засобів або носіїв інформації;
- забезпечує взаємодію Коледжу з Одеським національним технологічним університетом, Державною службою спеціального зв'язку та захисту інформації України, її територіальними органами, Національною поліцією України, кіберполіцією, іншими компетентними державними органами, власниками, розпорядниками та адміністраторами інформаційних систем у випадках і порядку, передбачених законодавством України;
- здійснює контроль за виконанням цього Положення та прийнятих на його виконання організаційно-розпорядчих документів.

2.8. Відповідальна особа є штатним працівником Коледжу, на якого наказом керівника Коледжу покладено виконання функцій з організації технічного захисту інформації та кібербезпеки. Відповідальна особа здійснює свою діяльність відповідно до законодавства України, цього Положення, наказів керівника Коледжу та інших локальних нормативних актів.

Виконання відповідальною особою функцій системного адміністрування окремих технічних засобів, інформаційних ресурсів, облікових записів, мережевого обладнання та програмного забезпечення допускається у разі покладення на неї відповідних функцій у встановленому в Коледжі порядку.

2.9. Відповідальна особа:

- бере участь у визначенні інформації, інформаційних ресурсів, систем, програмних і технічних засобів, які потребують захисту;
- організовує ведення та актуалізацію переліку інформаційних ресурсів, систем, електронних сервісів, комп'ютерної техніки та інших технічних засобів, що мають істотне значення для забезпечення діяльності Коледжу та потребують застосування заходів захисту;
- бере участь у визначенні категорій інформації, яка обробляється структурними підрозділами Коледжу, та необхідних заходів її захисту;
- готує пропозиції керівнику Коледжу щодо організаційних і технічних заходів із технічного захисту інформації та кібербезпеки;

- організовує впровадження та в межах наданих повноважень безпосередньо здійснює технічні заходи захисту інформації;
- бере участь в організації розмежування доступу до інформаційних ресурсів і технічних засобів;
- здійснює в межах наданих повноважень адміністрування засобів захисту інформації, мережевого обладнання, комп'ютерної техніки, програмного забезпечення, корпоративних облікових записів та інших інформаційних ресурсів;
- організовує та проводить періодичні перевірки стану захищеності комп'ютерної техніки, програмного забезпечення, мережевого обладнання та інших інформаційних ресурсів Коледжу;
- здійснює моніторинг актуальних кіберзагроз, відомостей про вразливості програмного забезпечення та рекомендацій компетентних державних органів у сфері кібербезпеки;
- організовує в межах повноважень виявлення, реєстрацію, первинне оцінювання, локалізацію та усунення наслідків кіберінцидентів;
- невідкладно інформує керівника Коледжу про кіберінциденти, які спричинили або можуть спричинити порушення конфіденційності, цілісності чи доступності інформації, істотне порушення роботи інформаційних ресурсів або інші значні негативні наслідки;
- готує пропозиції щодо необхідності повідомлення компетентних державних органів, власників, розпорядників та адміністраторів відповідних інформаційних систем про виявлені кіберінциденти;
- координує в межах наданих повноважень виконання заходів із резервного копіювання та відновлення інформації;
- контролює дотримання встановлених у Коледжі правил використання змінних носіїв інформації та підключення сторонніх технічних пристроїв до комп'ютерної техніки і мереж Коледжу;
- бере участь в організації захисту персональних даних, що обробляються в електронній формі, у межах компетенції з питань технічного захисту інформації та кібербезпеки;
- організовує впровадження заходів кібергігієни;
- бере участь в організації навчання та інформування працівників і здобувачів освіти з питань безпечного використання інформаційних технологій та протидії кіберзагрозам;
- консультує структурні підрозділи та працівників Коледжу з технічних і організаційних питань захисту інформації;
- готує пропозиції щодо придбання, впровадження, модернізації та використання програмних і технічних засобів захисту інформації;

- бере участь у розробленні локальних нормативних актів, інструкцій, процедур, планів заходів та інших документів з питань технічного захисту інформації та кібербезпеки;
- організовує ведення документації, передбаченої цим Положенням;
- взаємодіє в межах наданих повноважень із територіальними органами Держспецзв'язку, власниками, розпорядниками та адміністраторами інформаційних систем та іншими компетентними суб'єктами;
- здійснює інші функції у сфері технічного захисту інформації та кібербезпеки, покладені на неї законодавством України, наказами керівника Коледжу та локальними нормативними актами Коледжу.

2.10. Відповідальна особа має право:

- отримувати від структурних підрозділів і працівників інформацію, необхідну для виконання покладених на неї функцій, крім випадків обмеження доступу відповідно до закону;
- отримувати у встановленому порядку доступ до технічних засобів, програмного забезпечення, системних журналів, налаштувань та іншої технічної інформації в обсязі, необхідному для виконання покладених функцій;
- проводити планові та позапланові перевірки дотримання вимог цього Положення;
- вимагати припинення дій, що створюють безпосередню загрозу безпеці інформації, інформаційним ресурсам або технічним засобам Коледжу, та невідкладно інформувати про це керівника Коледжу;
- у разі виявлення безпосередньої загрози поширення шкідливого програмного забезпечення, компрометації облікових даних, несанкціонованого доступу або іншого кіберінциденту тимчасово обмежувати доступ до інформаційного ресурсу, відключати технічний засіб від мережі або вживати інших невідкладних заходів локалізації в межах наданих повноважень з обов'язковим невідкладним повідомленням керівника Коледжу;
- вносити керівнику Коледжу обов'язкові для розгляду пропозиції щодо усунення виявлених недоліків та порушень;
- ініціювати проведення службового розгляду, внутрішньої перевірки або створення комісії у разі виявлення істотного порушення вимог захисту інформації чи кіберінциденту;
- брати участь у плануванні закупівель комп'ютерної техніки, мережевого обладнання, програмного забезпечення та засобів захисту інформації шляхом надання рекомендацій щодо вимог безпеки;

- залучати за погодженням із керівником Коледжу інших працівників та, за потреби, зовнішніх фахівців до виконання окремих заходів у сфері технічного захисту інформації та кібербезпеки;
- підвищувати кваліфікацію з питань технічного захисту інформації та кібербезпеки відповідно до законодавства та можливостей Коледжу.

2.11. Відповідальна особа зобов’язана:

- діяти виключно в межах наданих повноважень;
- дотримуватися законодавства України, вимог цього Положення та інших локальних нормативних актів Коледжу;
- не розголошувати інформацію з обмеженим доступом та іншу інформацію, доступ до якої отримано у зв’язку з виконанням покладених функцій;
- не використовувати адміністративні повноваження з метою, не пов’язаною з виконанням службових обов’язків;
- застосовувати принцип мінімально необхідного доступу під час надання користувачам прав доступу;
- забезпечувати належне зберігання отриманих у зв’язку з виконанням функцій технічних відомостей, резервних копій, журналів подій, конфігураційних даних та інших матеріалів;
- документувати істотні кіберінциденти, результати перевірок та виявлені суттєві недоліки у порядку, визначеному цим Положенням;
- невідкладно повідомляти керівника Коледжу про обставини, які перешкоджають належному виконанню покладених функцій або створюють істотний ризик порушення безпеки інформації.

2.12. Керівники структурних підрозділів у межах своїх повноважень:

- забезпечують виконання вимог цього Положення працівниками відповідного структурного підрозділу;
- визначають та подають у встановленому порядку пропозиції щодо надання працівникам доступу до інформаційних ресурсів відповідно до їх посадових обов’язків;
- повідомляють відповідальну особу про прийняття працівників на роботу, переведення, зміну функціональних обов’язків, тривалу відсутність або припинення трудових відносин у випадках, коли такі обставини потребують надання, зміни, тимчасового обмеження чи припинення доступу до інформаційних ресурсів;
- забезпечують у межах компетенції належну організацію обробки та зберігання інформації у відповідному структурному підрозділі;
- не допускають надання працівникам надлишкових прав доступу до інформації та інформаційних ресурсів;

- забезпечують повідомлення відповідальної особи про виявлені кіберінциденти, підозрілі події, втрату носіїв інформації, компрометацію облікових даних та інші порушення вимог безпеки;
- сприяють проведенню перевірок стану захисту інформації та виконанню заходів щодо усунення виявлених недоліків;
- забезпечують участь працівників підрозділу у навчальних та інформаційних заходах із кібергігієни та кібербезпеки.

2.13. Працівники, які виконують функції адміністраторів ЄДЕБО та інших інформаційних систем, електронних сервісів або корпоративних облікових записів:

- здійснюють адміністрування виключно в межах наданих повноважень;
- забезпечують надання, зміну, блокування та припинення доступу користувачів відповідно до встановленого порядку та правил відповідної системи;
- застосовують доступні механізми автентифікації та захисту облікових записів;
- не передають іншим особам власні облікові дані, засоби автентифікації, КЕП, паролі та інші засоби доступу;
- забезпечують збереження конфіденційності адміністративної та іншої технічної інформації;
- повідомляють відповідальну особу про виявлені ознаки несанкціонованого доступу, компрометації облікових записів, порушення роботи системи та інші кіберінциденти;
- виконують вимоги законодавства України, цього Положення, локальних нормативних актів Коледжу та правила використання відповідної інформаційної системи.

2.14. Працівники Коледжу зобов’язані:

- дотримуватися вимог цього Положення та інших локальних нормативних актів з питань захисту інформації;
- використовувати інформаційні ресурси, технічні засоби, програмне забезпечення та електронні сервіси виключно в межах наданих повноважень та для виконання посадових обов’язків;
- забезпечувати збереження облікових даних, паролів, засобів автентифікації, КЕП та носіїв ключової інформації;
- не надавати іншим особам доступ до власних облікових записів;
- не встановлювати та не використовувати програмне забезпечення з порушенням законодавства, умов ліцензування або встановлених у Коледжі правил;

- не змінювати без належних повноважень налаштування засобів захисту інформації;
- дотримуватися встановленого порядку використання змінних носіїв та сторонніх технічних пристроїв;
- негайно повідомляти безпосереднього керівника та/або відповідальну особу про втрату пристрою чи носія інформації, підозру на компрометацію пароля, КЕП або іншого засобу автентифікації, виявлення шкідливого програмного забезпечення, фішингового повідомлення, несанкціонованого доступу чи іншої підозрілої події;
- проходити передбачені у Коледжі навчальні, інформаційні та інструктивні заходи з питань кібергігієни та кібербезпеки;
- виконувати законні вимоги відповідальної особи щодо усунення порушень вимог захисту інформації.

2.15. Здобувачі освіти під час використання комп'ютерної техніки, мережевого доступу та інших інформаційних ресурсів Коледжу зобов'язані:

- використовувати надані інформаційні ресурси відповідно до їх призначення;
- забезпечувати конфіденційність власних облікових даних;
- не здійснювати спроб несанкціонованого доступу до інформаційних ресурсів, облікових записів та технічних засобів інших користувачів;
- не створювати, не завантажувати, не поширювати та не запускати шкідливе програмне забезпечення;
- не вчиняти дій, спрямованих на порушення доступності, цілісності або конфіденційності інформаційних ресурсів;
- повідомляти працівника Коледжу, відповідального за відповідний інформаційний ресурс, та/або відповідальну особу про виявлені ознаки кіберінциденту;
- дотримуватися інших вимог цього Положення та правил використання відповідних інформаційних ресурсів.

2.16. Структурні підрозділи Коледжу взаємодіють із відповідальною особою шляхом:

- надання інформації, необхідної для визначення інформаційних ресурсів, технічних засобів та інформації, що потребує захисту;
- погодження в межах компетенції питань надання та припинення доступу до інформаційних ресурсів;
- повідомлення про кіберінциденти, технічні несправності та інші події, що можуть впливати на безпеку інформації;
- участі у перевірках, навчальних заходах, оцінюванні ризиків та виконанні заходів з усунення виявлених недоліків;

- виконання рішень керівника Коледжу та вимог локальних нормативних актів з питань технічного захисту інформації та кібербезпеки.

2.17. Надання доступу працівникам до інформаційних ресурсів здійснюється відповідно до посадових обов'язків, принципу мінімально необхідних повноважень, вимог законодавства та правил використання відповідної інформаційної системи.

Права доступу підлягають перегляду в разі зміни посадових обов'язків, переведення працівника, припинення трудових відносин, зміни функцій структурного підрозділу, виявлення надлишкових повноважень, кіберінциденту або інших обставин, що впливають на обґрунтованість наданого доступу.

Порядок управління доступом до конкретної зовнішньої інформаційної системи визначається також нормативно-правовими актами, регламентами та правилами її власника, розпорядника або адміністратора.

2.18. У Коледжі організовується ведення та періодичне актуалізування відомостей про:

- інформаційні ресурси та електронні сервіси, що використовуються в діяльності Коледжу;
- структурні підрозділи та категорії працівників, які здійснюють обробку персональних даних, службової та іншої інформації з обмеженим доступом;
- засоби електронної ідентифікації, КЕП та носії ключової інформації – у межах, необхідних для організації їх належного використання та обліку;
- заходи резервного копіювання інформації;
- виявлені істотні недоліки захисту та стан їх усунення;
- зареєстровані кіберінциденти.

2.19. Відповідальна особа не рідше одного разу на рік організовує внутрішнє оцінювання стану технічного захисту інформації та кібербезпеки Коледжу. Під час оцінювання враховуються, зокрема:

- зміни в переліку інформаційних ресурсів та технічних засобів;
- зміни в характері інформації, що обробляється;
- актуальні кіберзагрози та відомі вразливості;
- результати попередніх перевірок;
- зареєстровані кіберінциденти;
- стан управління доступом;
- стан оновлення програмного забезпечення та застосування засобів захисту;
- організація резервного копіювання та можливість відновлення інформації;
- дотримання правил використання змінних носіїв та сторонніх пристроїв;

- стан проведення заходів із кібергігієни та навчання користувачів;
- виконання рекомендацій і вимог компетентних державних органів у межах, установлених законодавством.

За результатами оцінювання відповідальна особа готує звіт, перелік виявлених недоліків або план заходів щодо вдосконалення стану захисту інформації та подає його керівнику Коледжу.

2.20. Планові внутрішні перевірки стану дотримання вимог цього Положення проводяться відповідно до плану роботи Коледжу або окремого плану заходів з питань технічного захисту інформації та кібербезпеки. Позапланові перевірки можуть проводитися:

- після виникнення істотного кіберінциденту;
- у разі виявлення ознак порушення вимог захисту інформації;
- після істотних змін інформаційної або технічної інфраструктури;
- за дорученням керівника Коледжу;
- у разі отримання відповідного запиту, припису, рекомендації або іншого документа компетентного державного органу в межах його повноважень.

2.21. За результатами перевірок та оцінювання стану технічного захисту інформації і кібербезпеки:

- визначаються виявлені недоліки та порушення;
- оцінюється необхідність застосування додаткових заходів захисту;
- визначаються відповідальні за виконання заходів;
- встановлюються строки усунення недоліків з урахуванням рівня ризику, складності та ресурсів, необхідних для їх усунення;
- здійснюється контроль виконання запланованих заходів.

2.22. У разі запровадження у Коледжі нової інформаційної системи, електронного сервісу, програмного продукту або істотної зміни способу обробки інформації структурний підрозділ – ініціатор такого впровадження – до початку використання відповідного ресурсу повідомляє відповідальну особу.

2.23. Питання щодо необхідності створення цільового профілю безпеки системи, проведення авторизації з безпеки, застосування відповідного базового профілю безпеки, оцінювання відповідності засобів захисту та виконання інших спеціальних вимог законодавства вирішуються щодо кожної конкретної системи окремо.

2.24. Взаємодія Коледжу з власниками, розпорядниками та адміністраторами зовнішніх інформаційних систем і сервісів здійснюється відповідно до законодавства України, договорів, регламентів, правил та умов використання відповідних систем.

2.25. Організація технічного захисту інформації та кібербезпеки здійснюється на постійній основі та підлягає перегляду і вдосконаленню з урахуванням:

- змін законодавства України;
- змін в організаційній структурі Коледжу;
- впровадження нових інформаційних технологій, систем і сервісів;
- зміни характеру та обсягів інформації, що обробляється;
- появи нових кіберзагроз і вразливостей;
- результатів перевірок, оцінювання стану захищеності та аналізу кіберінцидентів;
- рекомендацій та обов'язкових вимог компетентних державних органів.

3. ОБ'ЄКТИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ТА ОРГАНІЗАЦІЯ ЇХ ЗАХИСТУ

3.1. Об'єктами технічного захисту інформації та кіберзахисту у Коледжі є інформація, інформаційні ресурси, інформаційні, електронні інформаційно-комунікаційні системи, електронні сервіси, програмне забезпечення, комп'ютерна техніка, мережеве обладнання, носії інформації, засоби електронної ідентифікації та автентифікації, засоби кваліфікованого електронного підпису, резервні копії та інші інформаційні активи, що використовуються у діяльності Коледжу.

3.2. Захисту підлягає інформація незалежно від форми її подання, способу створення, обробки, передавання та зберігання, якщо необхідність її захисту встановлена законодавством України, умовами використання відповідної інформаційної системи або випливає з повноважень та законних інтересів Коледжу.

3.3. У Коледжі підлягають захисту, зокрема:

- персональні дані працівників, здобувачів освіти, вступників та інших фізичних осіб, що обробляються Коледжем на законних підставах;
- службова інформація – у разі її створення, одержання або обробки Коледжем та віднесення до службової інформації відповідно до законодавства України;
- інформація державних інформаційних ресурсів, доступ до якої надано Коледжу та його уповноваженим працівникам;
- кадрова, навчальна, методична, фінансова, бухгалтерська, договірна, управлінська та інша інформація, несанкціоноване знищення, зміна, блокування, копіювання, поширення або втрата якої може завдати шкоди правам фізичних осіб, діяльності Коледжу або інтересам держави;
- електронні документи, бази даних, робочі файли та резервні копії інформації;

- облікові дані користувачів, паролі, коди відновлення доступу, засоби багатофакторної автентифікації та інші дані, що використовуються для доступу до інформаційних ресурсів;
- особисті ключі кваліфікованого електронного підпису, інші ключові дані та засоби їх зберігання;
- конфігураційні дані, системні журнали, відомості про технічну інфраструктуру та інша інформація, розголошення або неправомірне використання якої може створити загрозу безпеці інформаційних ресурсів Коледжу.

3.4. До інформаційних ресурсів, систем та електронних сервісів, що використовуються Коледжем і потребують застосування відповідних заходів захисту, належать:

- Єдина державна електронна база з питань освіти (ЄДЕБО);
- система електронної взаємодії органів виконавчої влади (СЕВ ОВВ);
- корпоративна освітня платформа Google Workspace;
- інформаційні системи та електронні сервіси Державної казначейської служби України, Пенсійного фонду України, Державної податкової служби України та інших органів державної влади;
- системи електронного документообігу, бухгалтерського обліку, фінансової звітності, публічних закупівель, аукціонів та відкритих даних, що використовуються Коледжем, та інше програмне забезпечення, що використовується для виконання завдань структурних підрозділів;
- офіційні та корпоративні електронні поштові скриньки;
- вебсайт Коледжу та інші інформаційні ресурси, адміністрування яких здійснюється Коледжем або уповноваженими ним особами;
- інші інформаційні системи, програмні продукти та електронні сервіси, які впроваджуються або використовуються у діяльності Коледжу.

3.5. Використання Коледжем зовнішньої інформаційної системи або електронного сервісу не означає набуття Коледжем статусу власника чи розпорядника відповідної системи. Заходи захисту інформації під час використання таких систем забезпечуються Коледжем у межах його повноважень, технічних можливостей користувача системи та відповідальності за належне використання наданих облікових записів, технічних засобів, інформації, засобів автентифікації та електронного підпису.

3.6. До технічних засобів та компонентів інформаційної інфраструктури Коледжу, які потребують застосування заходів захисту, належать:

- стаціонарні та портативні комп’ютери, що використовуються працівниками;

- комп’ютерні робочі місця адміністраторів ЄДЕБО та інших інформаційних систем;
- мережеве та телекомунікаційне обладнання;
- засоби доступу до мережі Інтернет та бездротових мереж;
- змінні та зовнішні носії інформації;
- токени та інші носії особистих ключів КЕП;
- технічні засоби резервного копіювання та зберігання інформації;
- інші технічні засоби, на яких створюється, обробляється, передається або зберігається інформація, що підлягає захисту.

3.7. Застосування заходів захисту щодо конкретного інформаційного ресурсу, системи або технічного засобу визначається з урахуванням:

- правового режиму та значущості інформації, що обробляється;
- наслідків порушення конфіденційності, цілісності або доступності інформації;
- правового статусу Коледжу щодо відповідної системи;
- способу доступу до інформаційного ресурсу та кола користувачів;
- актуальних загроз, вразливостей і результатів оцінювання ризиків;
- вимог законодавства та правил використання відповідної системи.

Необхідність застосування базових або цільових профілів безпеки, проходження авторизації з безпеки, використання засобів технічного чи криптографічного захисту інформації з установленими законодавством документами про відповідність та виконання інших спеціальних вимог визначається окремо щодо кожної системи, на яку поширюються відповідні вимоги законодавства України.

3.8. Коледж забезпечує ведення та актуалізацію переліку інформаційних ресурсів, систем і сервісів, що використовуються в його діяльності.

3.9. Обробка персональних даних із використанням інформаційних технологій здійснюється виключно працівниками, яким такий доступ необхідний для виконання посадових обов’язків, з дотриманням вимог законодавства України про захист персональних даних та цього Положення.

Технічні та організаційні заходи захисту персональних даних повинні забезпечувати захист від випадкової втрати, знищення, незаконної обробки, несанкціонованого доступу, зміни, копіювання та поширення.

Передавання персональних даних іншим особам або надання доступу до них допускається лише за наявності правової підстави та з дотриманням установленого порядку.

3.10. Обробка службової інформації в електронній формі здійснюється з дотриманням вимог законодавства України щодо обліку, доступу, зберігання, передавання та захисту такої інформації.

3.11. Доступ до інформаційних ресурсів Коледжу надається відповідно до посадових обов'язків, навчальних потреб, установлених повноважень користувача та принципу мінімально необхідного доступу.

Кожний користувач несе відповідальність за дії, вчинені з використанням наданого йому облікового запису та засобів автентифікації, якщо інше не встановлено за результатами перевірки обставин компрометації або несанкціонованого використання таких засобів.

3.12. Робочі комп'ютери, на яких здійснюється обробка персональних даних, службової інформації, інформації державних інформаційних ресурсів або використання КЕП, повинні розміщуватися та використовуватися таким чином, щоб унеможливити неконтрольований доступ сторонніх осіб до інформації, засобів автентифікації та носіїв ключової інформації.

Доступ сторонніх осіб до приміщень із комп'ютерними робочими місцями, на яких систематично обробляється інформація з обмеженим доступом, контролюється відповідальними працівниками відповідних структурних підрозділів.

Після завершення роботи приміщення, обладнані засобами охоронної сигналізації, зачиняються та передаються під охорону відповідно до встановленого у Коледжі порядку.

3.13. Використання особистих комп'ютерів, мобільних пристроїв та інших технічних засобів працівників для обробки інформації з обмеженим доступом допускається лише у випадках, коли це прямо дозволено законодавством, правилами відповідної інформаційної системи та локальними актами Коледжу і забезпечено необхідний рівень захисту інформації.

3.14. Носії інформації, засоби КЕП, резервні копії та інші інформаційні активи повинні зберігатися у спосіб, що унеможливлює неконтрольований доступ, втрату, викрадення, підміну або неправомірне копіювання інформації.

Працівник, якому передано носій інформації, токен або інший засіб доступу, зобов'язаний забезпечувати його належне зберігання та невідкладно повідомляти про втрату, викрадення, пошкодження або підозру на компрометацію.

3.15. Впровадження нового інформаційного ресурсу, програмного продукту, електронного сервісу або технічного рішення, призначеного для систематичної обробки інформації Коледжу, здійснюється з попереднім урахуванням вимог до захисту інформації.

3.16. У разі припинення використання інформаційного ресурсу, технічного засобу або носія інформації повинні бути вжиті заходи щодо:

- припинення або блокування доступу користувачів;
- збереження інформації, що підлягає подальшому зберіганню;
- перенесення інформації до іншого інформаційного ресурсу, якщо це необхідно;
- видалення інформації з урахуванням установлених строків її зберігання;
- знищення, очищення або підготовки носіїв інформації до повторного використання у спосіб, що мінімізує ризик несанкціонованого відновлення захищеної інформації;
- припинення дії, блокування або відкликання засобів доступу та електронної ідентифікації, якщо це необхідно.

3.17. Стан об'єктів технічного захисту інформації та кіберзахисту, склад інформаційних ресурсів, характер інформації, що обробляється, та достатність застосованих заходів захисту підлягають періодичному перегляду відповідальною особою. За результатами перегляду відповідальна особа за необхідності подає керівникові Коледжу пропозиції щодо зміни організаційних і технічних заходів захисту інформації.

4. ЗАХОДИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКИ

4.1. Заходи технічного захисту інформації та кібербезпеки у Коледжі здійснюються відповідно до законодавства України, цього Положення, інших локальних нормативних актів Коледжу, вимог власників, розпорядників та адміністраторів інформаційних систем, а також з урахуванням характеру інформації, актуальних кіберзагроз і наявних ризиків.

Заходи захисту повинні бути спрямовані на запобігання порушенню конфіденційності, цілісності та доступності інформації, несанкціонованому доступу до інформаційних ресурсів, втраті, знищенню, неправомірній зміні або поширенню інформації, порушенню роботи інформаційних систем і технічних засобів.

4.2. У Коледжі забезпечується здійснення організаційних і технічних заходів захисту інформації, зокрема щодо:

- управління доступом до інформаційних ресурсів;
- захисту облікових записів та засобів автентифікації;
- безпечного використання комп'ютерної техніки та програмного забезпечення;
- захисту від шкідливого програмного забезпечення;

- управління вразливостями та оновлення програмного забезпечення;
- захисту мережевої інфраструктури та електронних комунікацій;
- безпечного використання електронної пошти, хмарних сервісів та зовнішніх інформаційних систем;
- захисту носіїв інформації та засобів КЕП;
- резервного копіювання та відновлення інформації;
- фізичного захисту технічних засобів та місць обробки інформації;
- моніторингу подій, що можуть свідчити про порушення безпеки;
- підвищення обізнаності користувачів з питань кібергігієни та кібербезпеки.

Конкретний склад і обсяг заходів визначаються з урахуванням вимог законодавства, результатів оцінювання ризиків, технічних можливостей Коледжу та правового статусу Коледжу щодо відповідної системи.

4.3. Доступ до інформаційних ресурсів надається користувачам лише в обсязі, необхідному для виконання посадових обов'язків, освітньої діяльності або інших правомірних завдань.

Права доступу підлягають перегляду в разі зміни посадових або функціональних обов'язків користувача, переведення, припинення трудових відносин, завершення навчання, втрати необхідності у використанні відповідного ресурсу, виникнення кіберінциденту або інших обставин, що впливають на обґрунтованість наданого доступу.

4.4. Для доступу до інформаційних ресурсів використовуються персональні облікові записи та засоби автентифікації, крім випадків, коли інший порядок використання облікових записів передбачений функціональними особливостями відповідної системи.

Користувачі зобов'язані забезпечувати конфіденційність паролів та інших засобів автентифікації, не передавати їх іншим особам і невідкладно повідомляти відповідальну особу або адміністратора відповідної системи про підозру щодо їх компрометації. Паролі повинні відповідати вимогам відповідної інформаційної системи та встановленим у Коледжі мінімальним вимогам безпеки.

Для інформаційних ресурсів, що підтримують багатофакторну автентифікацію, вона застосовується з урахуванням рівня ризику, характеру інформації, прав користувача та технічних можливостей відповідної системи.

4.5. Працівники використовують комп'ютерну техніку та програмне забезпечення Коледжу відповідно до їх призначення, посадових обов'язків і встановлених вимог безпеки.

Не допускаються без належного дозволу:

- встановлення програмного забезпечення;
- відключення, видалення або зміна налаштувань засобів захисту;
- зміна системних і мережевих налаштувань, якщо такі дії не належать до повноважень користувача;
- використання програмного забезпечення, одержаного з ненадійних джерел або з порушенням законодавства та умов ліцензування;
- надання стороннім особам неконтрольованого доступу до технічних засобів Коледжу.

4.6. На комп'ютерній техніці Коледжу застосовуються передбачені операційними системами, програмним забезпеченням та іншими технічними засобами механізми захисту. Залежно від призначення технічного засобу, характеру інформації та наявних ризиків забезпечуються:

- захист доступу до операційної системи;
- блокування робочого сеансу в разі залишення робочого місця без нагляду;
- використання засобів захисту від шкідливого програмного забезпечення;
- своєчасне встановлення оновлень безпеки;
- обмеження використання адміністративних прав;
- захист даних на носіях інформації, у тому числі із застосуванням шифрування, якщо це необхідно та технічно можливо.

4.7. У Коледжі забезпечується захист від шкідливого програмного забезпечення шляхом використання штатних засобів захисту операційних систем та/або іншого програмного забезпечення відповідного призначення, регулярного оновлення таких засобів, обмеження запуску небезпечного програмного забезпечення та дотримання користувачами вимог кібергігієни.

У разі виявлення ознак зараження шкідливим програмним забезпеченням користувач повинен припинити дії, які можуть сприяти його поширенню, та невідкладно повідомити відповідальну особу.

4.8. Операційні системи, прикладне програмне забезпечення, веббраузери, засоби захисту інформації та інші програмні компоненти повинні підтримуватися в актуальному стані.

Оновлення безпеки встановлюються у розумні строки з урахуванням критичності виявлених вразливостей, технічної можливості встановлення оновлення та необхідності забезпечення стабільної роботи програмного забезпечення.

4.9. Захист мережевої інфраструктури та електронних комунікацій Коледжу здійснюється шляхом застосування доступних організаційних і технічних заходів, спрямованих на обмеження несанкціонованого доступу, зменшення

можливості поширення шкідливого програмного забезпечення та захист інформації під час її передавання.

Безпека бездротових мереж забезпечується використанням належних засобів автентифікації та шифрування, захистом адміністративного доступу до мережевого обладнання та своєчасним оновленням його програмного забезпечення.

4.10. Використання електронної пошти, мережевих освітніх платформ, хмарних технологій та інших електронних сервісів здійснюється відповідно до їх призначення, вимог законодавства, цього Положення та правил використання відповідних сервісів.

Працівники та здобувачі освіти повинні дотримуватися обережності під час отримання електронних повідомлень, відкриття вкладень, переходу за посиланнями та надання облікових даних.

4.11. Використання змінних носіїв інформації та підключення сторонніх технічних пристроїв здійснюються з дотриманням установлених у Коледжі вимог безпеки. На носіях інформації не повинна зберігатися інформація, яка не є необхідною для виконання службових або навчальних завдань. Для захисту інформації на змінних носіях за необхідності застосовуються засоби шифрування та інші доступні заходи захисту.

4.12. Засоби КЕП та інші засоби електронної ідентифікації використовуються виключно особами, яким вони належать або на законних підставах надані для використання.

Передавання особистих ключів, паролів, кодів доступу та інших засобів контролю доступу до особистих ключів іншим особам не допускається.

Зберігання, використання, блокування, скасування та поновлення сертифікатів відкритих ключів здійснюються відповідно до законодавства України та вимог надавачів відповідних електронних довірчих послуг. У разі втрати носія особистого ключа або підозри щодо його компрометації працівник зобов’язаний невідкладно вжити передбачених законодавством і правилами надавача електронних довірчих послуг заходів та повідомити відповідальну особу і безпосереднього керівника.

4.13. Резервне копіювання здійснюється щодо інформації, втрата, пошкодження або недоступність якої може істотно вплинути на діяльність Коледжу, якщо створення резервних копій належить до технічних можливостей і повноважень Коледжу.

Перелік інформації, що підлягає резервному копіюванню, періодичність створення копій, місця їх зберігання, строки зберігання та відповідальні особи визначаються з урахуванням значущості інформації, характеру її

використання та результатів оцінювання ризиків. Резервні копії повинні бути захищені від несанкціонованого доступу, випадкового знищення та впливу подій, які можуть одночасно призвести до втрати основної інформації та її резервних копій. Можливість відновлення інформації з резервних копій підлягає періодичній перевірці.

4.14. Фізичний захист комп'ютерної техніки, носіїв інформації, засобів КЕП, мережевого обладнання та інших технічних засобів забезпечується з урахуванням характеру інформації, що на них обробляється або зберігається, та ризиків несанкціонованого фізичного доступу.

Ключі, токени, змінні носії та інші засоби доступу не повинні залишатися без належного нагляду або зберігатися у місцях, доступних стороннім особам.

4.15. Під час використання зовнішніх інформаційних систем і сервісів Коледж забезпечує виконання заходів захисту в межах наданих йому повноважень та технічних можливостей користувача відповідної системи.

4.16. У Коледжі здійснюється моніторинг стану захищеності інформаційних ресурсів у межах наявних технічних можливостей та повноважень.

Моніторинг може включати перевірку стану оновлення програмного забезпечення, функціонування засобів захисту, налаштувань доступу, використання адміністративних прав, наявності відомих вразливостей, підозрілих подій та інших обставин, що можуть впливати на безпеку інформації.

Обсяг моніторингу визначається відповідальною особою з урахуванням законодавства, характеру інформаційних ресурсів, рівня ризиків та технічних можливостей Коледжу.

4.17. Працівники та здобувачі освіти, які використовують інформаційні ресурси Коледжу, повинні дотримуватися базових правил кібергігієни.

4.18. Застосування конкретних технічних, програмних, криптографічних та інших засобів захисту здійснюється відповідно до вимог законодавства України.

4.19. Заходи технічного захисту інформації та кібербезпеки підлягають перегляду в разі:

- зміни вимог законодавства України;
- зміни складу інформаційних ресурсів, технічної інфраструктури або способів обробки інформації;
- виникнення кіберінцидентів, які свідчать про недостатність застосованих заходів захисту;
- виявлення нових істотних загроз або вразливостей;

- отримання обов’язкових вимог або рекомендацій компетентних державних органів;
- встановлення за результатами внутрішнього оцінювання недостатності або неефективності застосованих заходів.

За результатами перегляду відповідальна особа готує пропозиції щодо вдосконалення організаційних і технічних заходів захисту інформації та подає їх керівникові Коледжу для розгляду.

5. ПОРЯДОК РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ, МОНІТОРИНГ ТА КОНТРОЛЬ СТАНУ КІБЕРБЕЗПЕКИ

5.1. У Коледжі забезпечуються виявлення, реєстрація, оцінювання та реагування на кіберінциденти, а також моніторинг і контроль стану технічного захисту інформації та кібербезпеки відповідно до законодавства України, цього Положення та інших локальних нормативних актів Коледжу.

5.2. Кіберінцидентами або подіями, що потребують перевірки, можуть бути, зокрема:

- несанкціонований доступ до інформації, облікового запису, інформаційного ресурсу або технічного засобу;
- втрата, викрадення або компрометація засобів автентифікації, КЕП, технічних засобів чи носіїв інформації;
- виявлення шкідливого програмного забезпечення або ознак його функціонування;
- порушення конфіденційності, цілісності або доступності інформації;
- порушення нормального функціонування інформаційного ресурсу внаслідок кібератаки або інших протиправних дій;
- інші події, що створюють або можуть створити загрозу безпеці інформації та інформаційних ресурсів Коледжу.

5.3. Працівник або здобувач освіти, який виявив ознаки кіберінциденту чи іншу підозрілу подію, повинен невідкладно повідомити відповідальну особу, адміністратора відповідного інформаційного ресурсу або працівника Коледжу, відповідального за організацію відповідного процесу.

Особа, яка виявила кіберінцидент, не повинна самостійно видаляти файли, змінювати налаштування програмного забезпечення, знищувати електронні повідомлення, журнали подій або інші відомості, які можуть мати значення для встановлення причин та обставин інциденту, крім випадків, коли невідкладні дії необхідні для припинення безпосередньої загрози.

5.4. Відповідальна особа після отримання повідомлення про кіберінцидент у межах своїх повноважень:

- здійснює первинне оцінювання події та її можливих наслідків;
- організовує або здійснює невідкладні заходи з локалізації інциденту;
- вживає заходів для збереження доступних відомостей про обставини інциденту;
- інформує керівника Коледжу про істотні кіберінциденти;
- організовує відновлення належного функціонування інформаційних ресурсів у межах повноважень Коледжу;
- готує пропозиції щодо усунення причин інциденту та запобігання його повторенню.

5.5. Реагування на кіберінцидент здійснюється з урахуванням характеру події, масштабу її впливу, виду інформації, якої вона стосується, можливих наслідків для фізичних осіб, діяльності Коледжу та інформаційних ресурсів.

5.6. Істотні кіберінциденти підлягають реєстрації у журналі реєстрації кіберінцидентів. Реєстрація повинна забезпечувати можливість установлення основних обставин події, вжитих заходів реагування, наслідків інциденту та результатів його усунення.

5.7. Рішення про необхідність повідомлення Державної служби спеціального зв'язку та захисту інформації України, її територіального органу, Національної поліції України, кіберполіції, власника, розпорядника або адміністратора відповідної інформаційної системи чи іншого компетентного суб'єкта приймається відповідно до вимог законодавства України та з урахуванням характеру і наслідків кіберінциденту.

Відповідальна особа готує керівникові Коледжу пропозиції щодо такого повідомлення та забезпечує взаємодію з відповідними суб'єктами в межах наданих повноважень.

5.8. Після завершення реагування на істотний кіберінцидент відповідальна особа за необхідності проводить аналіз його причин, наслідків та ефективності вжитих заходів.

5.9. Моніторинг стану технічного захисту інформації та кібербезпеки здійснюється відповідальною особою в межах повноважень і наявних технічних можливостей Коледжу.

5.10. Контроль стану технічного захисту інформації та кібербезпеки здійснюється шляхом проведення внутрішніх перевірок, аналізу виявлених кіберінцидентів, оцінювання виконання встановлених заходів захисту та контролю усунення виявлених недоліків.

Періодичність і обсяг контрольних заходів визначаються з урахуванням характеру інформаційних ресурсів, рівня ризиків, змін інформаційної інфраструктури та результатів попередніх перевірок.

5.11. За результатами моніторингу, перевірок або аналізу кіберінцидентів відповідальна особа інформує директора Коледжу про істотні недоліки та за необхідності подає пропозиції щодо їх усунення і вдосконалення заходів технічного захисту інформації та кібербезпеки. Виявлені недоліки усуваються з урахуванням рівня ризику, можливих наслідків, технічної складності та наявних ресурсів Коледжу.

6. ПРАВА, ОБОВ'ЯЗКИ ТА ВІДПОВІДАЛЬНІСТЬ УЧАСНИКІВ СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКИ

6.1. Учасниками системи технічного захисту інформації та кібербезпеки Коледжу є посадові особи, працівники, адміністратори інформаційних систем та інших інформаційних ресурсів, здобувачі освіти, а також інші особи, яким у встановленому порядку надано доступ до інформаційних ресурсів або технічних засобів Коледжу.

Права, обов'язки та відповідальність учасників визначаються законодавством України, цим Положенням, іншими локальними нормативними актами Коледжу, посадовими обов'язками та правилами використання відповідних інформаційних систем.

6.2. Учасники системи технічного захисту інформації та кібербезпеки мають право:

- отримувати в межах своїх повноважень доступ до інформаційних ресурсів і технічних засобів, необхідних для виконання посадових, службових, освітніх або інших правомірних завдань;
- отримувати інформацію, роз'яснення та рекомендації щодо вимог безпечного використання інформаційних ресурсів і технічних засобів;
- повідомляти про виявлені недоліки, вразливості, кіберінциденти та інші обставини, що можуть впливати на стан захисту інформації;
- подавати пропозиції щодо вдосконалення заходів технічного захисту інформації та кібербезпеки;
- брати участь у навчальних та інформаційних заходах з питань кібербезпеки і кібергігієни.

6.3. Учасники системи технічного захисту інформації та кібербезпеки зобов'язані:

- дотримуватися вимог законодавства України, цього Положення та інших локальних нормативних актів Коледжу з питань захисту інформації;

- використовувати інформаційні ресурси, програмне забезпечення, технічні засоби та надані права доступу виключно з правомірною метою та в межах наданих повноважень;
- забезпечувати належне використання та збереження засобів автентифікації, КЕП, носіїв інформації та інших наданих їм засобів доступу;
- не допускати умисного створення загроз безпеці інформації, втручання в роботу інформаційних ресурсів або обходу встановлених засобів захисту;
- невідкладно повідомляти про виявлені кіберінциденти, втрату або компрометацію засобів доступу та інші події, що можуть створити загрозу безпеці інформації;
- сприяти проведенню заходів реагування на кіберінциденти, внутрішніх перевірок та усуненню виявлених порушень у межах своїх повноважень;
- виконувати законні вимоги керівника Коледжу, відповідальної особи та інших уповноважених осіб з питань захисту інформації.

6.4. Керівник Коледжу, відповідальна особа, керівники структурних підрозділів, адміністратори інформаційних систем та інші посадові особи виконують повноваження і несуть відповідальність за організацію та здійснення заходів технічного захисту інформації і кібербезпеки в межах компетенції, визначеної законодавством України, цим Положенням, наказами керівника Коледжу та іншими локальними нормативними актами Коледжу.

Покладення окремих функцій з технічного захисту інформації та кібербезпеки на відповідальну особу не звільняє інших посадових осіб і працівників від виконання покладених на них обов’язків щодо захисту інформації.

6.5. Керівники структурних підрозділів несуть відповідальність у межах своїх повноважень за належну організацію роботи з інформацією у відповідних підрозділах, дотримання працівниками встановлених вимог захисту інформації та своєчасне інформування про обставини, що можуть впливати на стан її захищеності.

6.6. Користувачі інформаційних ресурсів несуть відповідальність за дотримання встановлених правил доступу та безпечного використання інформації, облікових записів, технічних засобів, носіїв інформації, КЕП та інших засобів, наданих їм для виконання посадових, службових або освітніх завдань.

Користувач несе відповідальність за умисне передавання іншим особам власних засобів доступу, неправомірне використання наданих повноважень та інші винні дії або бездіяльність відповідно до законодавства України.

6.7. Особи, яким у зв’язку з виконанням посадових, службових або інших обов’язків став доступним зміст персональних даних, службової інформації або іншої інформації з обмеженим доступом, зобов’язані не допускати її неправомірного розголошення, використання, копіювання, передавання або надання доступу до неї іншим особам.

Обов’язок щодо нерозголошення інформації з обмеженим доступом зберігається після припинення трудових відносин, завершення навчання або припинення інших підстав доступу до такої інформації у випадках та межах, установлених законодавством України.

6.8. Порушеннями вимог цього Положення є винні дії або бездіяльність, що полягають у невиконанні чи неналежному виконанні встановлених вимог технічного захисту інформації та кібербезпеки.

До таких порушень можуть належати:

- неправомірне отримання або надання доступу до інформаційних ресурсів;
- передавання іншим особам засобів автентифікації або КЕП;
- умисне відключення, обхід або порушення роботи встановлених засобів захисту;
- неправомірне розголошення, копіювання, зміна, видалення або поширення інформації;
- приховування відомого кіберінциденту або несвоєчасне повідомлення про нього, якщо особа була зобов’язана здійснити таке повідомлення;
- невиконання законних вимог щодо усунення виявлених порушень та недоліків;
- інші порушення законодавства України у сфері технічного захисту інформації та кібербезпеки.

6.9. Особи, винні у порушенні законодавства у сфері захисту інформації, кібербезпеки, захисту персональних даних та вимог цього Положення, можуть бути притягнуті до дисциплінарної, цивільно-правової, адміністративної або кримінальної відповідальності відповідно до чинного законодавства України.

Застосування заходів відповідальності здійснюється виключно за наявності встановлених законодавством підстав і з дотриманням передбаченої законом процедури.

Притягнення особи до відповідальності не звільняє від обов’язку припинити порушення, усунути його наслідки та вжити заходів щодо недопущення повторного порушення.

6.10. У разі виявлення ознак порушення вимог цього Положення керівник Коледжу в межах своїх повноважень може прийняти рішення про проведення внутрішньої перевірки, витребування письмових пояснень, створення комісії або вжиття інших передбачених законодавством заходів для встановлення обставин події.

6.11. У разі встановлення ознак адміністративного чи кримінального правопорушення, істотного порушення прав суб’єктів персональних даних або інших обставин, що відповідно до законодавства потребують повідомлення компетентних державних органів чи інших суб’єктів, Коледж забезпечує вжиття відповідних заходів у встановленому законодавством порядку.

6.12. Обмеження, тимчасове блокування або припинення доступу особи до інформаційного ресурсу може застосовуватися з метою припинення безпосередньої загрози безпеці інформації, локалізації кіберінциденту, запобігання подальшому порушенню або у зв'язку з припиненням підстав для доступу.

6.13. Контроль за дотриманням прав, виконанням обов'язків та застосуванням положень про відповідальність у сфері технічного захисту інформації та кібербезпеки здійснюється керівником Коледжу, відповідальною особою та іншими уповноваженими посадовими особами в межах визначених повноважень.

Рішення та заходи, що приймаються у зв'язку з порушенням вимог захисту інформації, повинні бути законними, обґрунтованими та пропорційними характеру порушення і його наслідкам.

7. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

7.1. Це Положення затверджується Педагогічною радою Коледжу та вводиться в дію наказом керівника Коледжу.

7.2. Положення є обов'язковим для виконання всіма працівниками, здобувачами освіти та іншими особами в частині, що стосується наданого їм доступу до інформаційних ресурсів і технічних засобів Коледжу.

7.3. Зміни та доповнення до цього Положення вносяться у порядку, установленому для його затвердження, з урахуванням змін законодавства України, інформаційної інфраструктури Коледжу та характеру інформації, що обробляється.

7.4. Питання у сфері технічного захисту інформації та кібербезпеки, не врегульовані цим Положенням, вирішуються відповідно до законодавства України, інших локальних нормативних актів Коледжу та вимог, правил і регламентів відповідних інформаційних систем.

7.5. Додатки до цього Положення, затверджені разом із ним, є його невід'ємною частиною.

Розглянуто та схвалено
на засіданні Методичної ради
ВСП «ОТФК ОНТУ»
протокол № 11 від 10.06.2026 р.
Голова методичної ради

Юліан СУЛІМА

Положення розроблено робочою групою коледжу у складі:

Заст. директора з НМР,
викладач-методист _____ Юліан СУЛІМА

Заст. директор з ВР та СП,
викладач-методист _____ Тетяна КОПАЙГОРОДСЬКА

Зав. відділення
комп'ютерних систем _____ Катерина КРАСНОКУТСЬКА

Відповідальна особа за
технічний захист інформації
та кібербезпеку від коледжу _____ Дмитро ДЖАБРАЇЛОВ

Головний бухгалтер
коледжу _____ Анна ПЯТНІЧЕНКО

Юрисконсульт коледжу _____ Максим ХРУЛЬОВ

Голова ради студентського
самоврядування коледжу _____ Олена СЕРЕДА

ДОДАТКИ

ДОДАТОК 1. ПЕРЕЛІК ІНФОРМАЦІЙНИХ РЕСУРСІВ, СИСТЕМ ТА ЕЛЕКТРОННИХ СЕРВІСІВ, ЩО ВИКОРИСТОВУЮТЬСЯ У КОЛЕДЖІ

1. Цей Перелік призначений для обліку основних інформаційних ресурсів, інформаційних систем, програмних продуктів та електронних сервісів, що використовуються у діяльності Коледжу та потребують застосування організаційних і технічних заходів захисту інформації.

2. Перелік ведеться та актуалізується відповідальною особою за технічний захист інформації та кібербезпеку у взаємодії з керівниками структурних підрозділів та працівниками, які адмініструють або використовують відповідні інформаційні ресурси.

3. До Переліку включаються інформаційні ресурси, системи та електронні сервіси, які використовуються для здійснення освітньої, управлінської, кадрової, фінансово-господарської та іншої діяльності Коледжу.

4. Відомості Переліку переглядаються та за необхідності актуалізуються у разі впровадження нового інформаційного ресурсу, припинення його використання, істотної зміни способу доступу або характеру інформації, що обробляється.

5. У разі використання нового інформаційного ресурсу, системи або електронного сервісу відповідальна особа вносить відповідні відомості до Переліку після отримання необхідної інформації від структурного підрозділу – користувача такого ресурсу.

6. Виключення інформаційного ресурсу з Переліку здійснюється після припинення його використання Коледжем та виконання необхідних заходів щодо припинення доступу, збереження, перенесення або видалення інформації відповідно до законодавства України та цього Положення.

7. Перелік ведеться в електронній та/або паперовій формі. Актуальна редакція Переліку зберігається відповідальною особою.

8. Зміни до Переліку, що не змінюють зміст Положення та стосуються лише актуалізації відомостей про інформаційні ресурси, системи, сервіси, способи доступу, відповідальних осіб або резервне копіювання, не потребують внесення змін до самого Положення.

ПЕРЕЛІК ІНФОРМАЦІЙНИХ РЕСУРСІВ

№ 1	
Найменування інформаційного ресурсу, системи або сервісу	Єдина державна електронна база з питань освіти (ЄДЕБО)
Основне призначення	Облік даних у сфері освіти та виконання передбачених законодавством операцій
Структурні підрозділи / категорії користувачів	Адміністратори ЄДЕБО
Основні категорії інформації, що обробляється	Дані здобувачів освіти, вступників, працівників та інша інформація відповідно до функціоналу системи
Адміністрування або відповідальна особа з боку Коледжу	Адміністратори ЄДЕБО
Спосіб доступу та автентифікації	Персональні облікові записи, засоби автентифікації відповідно до вимог ЄДЕБО

№ 2	
Найменування інформаційного ресурсу, системи або сервісу	Система електронної взаємодії органів виконавчої влади (СЕВ ОВВ)
Основне призначення	Електронна взаємодія та обмін електронними документами
Структурні підрозділи / категорії користувачів	Уповноважені працівники
Основні категорії інформації, що обробляється	Електронні документи та пов’язані з ними дані
Адміністрування або відповідальна особа з боку Коледжу	Уповноважені працівники
Спосіб доступу та автентифікації	Облікові записи, КЕП та інші засоби відповідно до вимог системи

№ 3	
Найменування інформаційного ресурсу, системи або сервісу	Google Workspace
Основне призначення	Забезпечення освітньої діяльності
Структурні підрозділи / категорії користувачів	Педагогічні працівники, здобувачі освіти
Основні категорії інформації, що обробляється	Освітні матеріали та інша інформація, що обробляється в межах використання платформи
Адміністрування або відповідальна особа з боку Коледжу	Адміністратор Google Workspace
Спосіб доступу та автентифікації	Корпоративні облікові записи та засоби автентифікації платформи

№ 4	
Найменування інформаційного ресурсу, системи або сервісу	Електронні сервіси Державної казначейської служби України
Основне призначення	Казначейське обслуговування та подання фінансової звітності
Структурні підрозділи / категорії користувачів	Бухгалтерія
Основні категорії інформації, що обробляється	Фінансова, бухгалтерська та інша інформація відповідно до функціоналу сервісів
Адміністрування або відповідальна особа з боку Коледжу	Уповноважені працівники
Спосіб доступу та автентифікації	Засоби доступу, КЕП, токени відповідно до вимог сервісів

№ 5	
Найменування інформаційного ресурсу, системи або сервісу	Вчасно.ЕДО
Основне призначення	Електронний документообіг
Структурні підрозділи / категорії користувачів	Бухгалтерія
Основні категорії інформації, що обробляється	Електронні документи та пов’язані з ними дані
Адміністрування або відповідальна особа з боку Коледжу	Уповноважені працівники
Спосіб доступу та автентифікації	Облікові записи, КЕП та інші засоби відповідно до правил сервісу

№ 6	
Найменування інформаційного ресурсу, системи або сервісу	E-Tender
Основне призначення	Проведення операцій у сфері публічних закупівель, продажів та оренди
Структурні підрозділи / категорії користувачів	Бухгалтерія
Основні категорії інформації, що обробляється	Документи та дані, пов’язані з використанням системи
Адміністрування або відповідальна особа з боку Коледжу	Уповноважені працівники
Спосіб доступу та автентифікації	Засоби доступу та автентифікації відповідно до правил системи

№ 7	
Найменування інформаційного ресурсу, системи або сервісу	Є-data
Основне призначення	Робота з інформацією у сфері використання публічних коштів
Структурні підрозділи / категорії користувачів	Бухгалтерія
Основні категорії інформації, що обробляється	Фінансова та інша інформація відповідно до функціоналу системи
Адміністрування або відповідальна особа з боку Коледжу	Уповноважені працівники
Спосіб доступу та автентифікації	Засоби доступу відповідно до правил системи

№ 8	
Найменування інформаційного ресурсу, системи або сервісу	Ispro
Основне призначення	Автоматизація бухгалтерського обліку та управління
Структурні підрозділи / категорії користувачів	Бухгалтерія
Основні категорії інформації, що обробляється	Фінансова та бухгалтерська інформація
Адміністрування або відповідальна особа з боку Коледжу	Уповноважені працівники
Спосіб доступу та автентифікації	Засоби доступу відповідно до правил системи

№ 9	
Найменування інформаційного ресурсу, системи або сервісу	Програмний комплекс «Фіндокументи»
Основне призначення	Формування та обробка фінансових документів
Структурні підрозділи / категорії користувачів	Бухгалтерія
Основні категорії інформації, що обробляється	Фінансова та бухгалтерська інформація
Адміністрування або відповідальна особа з боку Коледжу	Уповноважені працівники
Спосіб доступу та автентифікації	Засоби доступу відповідно до правил системи

№ 10	
Найменування інформаційного ресурсу, системи або сервісу	M.E.Doc
Основне призначення	Формування, підписання та подання електронної звітності
Структурні підрозділи / категорії користувачів	Бухгалтерія
Основні категорії інформації, що обробляється	Фінансова, податкова, персональна та інша інформація відповідно до функціоналу програми
Адміністрування або відповідальна особа з боку Коледжу	Уповноважені працівники
Спосіб доступу та автентифікації	Облікові записи, КЕП та інші засоби автентифікації

№ 11	
Найменування інформаційного ресурсу, системи або сервісу	Електронні сервіси Пенсійного фонду України та Державної податкової служби України
Основне призначення	Виконання кадрових, податкових та інших передбачених законодавством процедур
Структурні підрозділи / категорії користувачів	Відділ кадрів, бухгалтерія
Основні категорії інформації, що обробляється	Персональні дані, кадрова, податкова та інша інформація
Адміністрування або відповідальна особа з боку Коледжу	Уповноважені працівники
Спосіб доступу та автентифікації	Засоби доступу та автентифікації відповідно до вимог сервісів

№ 12	
Найменування інформаційного ресурсу, системи або сервісу	Офіційні електронні поштові скриньки Коледжу та структурних підрозділів
Основне призначення	Службове електронне листування
Структурні підрозділи / категорії користувачів	Адміністрація, канцелярія, структурні підрозділи та уповноважені працівники
Основні категорії інформації, що обробляється	Службове листування та інша інформація, що передається електронною поштою
Адміністрування або відповідальна особа з боку Коледжу	Працівники, яким надано доступ до відповідних скриньок
Спосіб доступу та автентифікації	Облікові записи та паролі

№ 13	
Найменування інформаційного ресурсу, системи або сервісу	Офіційний вебсайт Коледжу
Основне призначення	Оприлюднення інформації та інформаційне забезпечення діяльності Коледжу
Структурні підрозділи / категорії користувачів	Уповноважені працівники
Основні категорії інформації, що обробляється	Публічна інформація, матеріали вебсайту
Адміністрування або відповідальна особа з боку Коледжу	Адміністратор вебсайту
Спосіб доступу та автентифікації	Обліковий запис адміністратора та засоби автентифікації

№ 14	
Найменування інформаційного ресурсу, системи або сервісу	Програмний комплекс StrikePlagiarism
Основне призначення	Перевірка робіт здобувачів освіти та науко-методичних розробок педагогічних працівників на наявність ознак академічного плагіату
Структурні підрозділи / категорії користувачів	Уповноважена особа від Коледжу за дотримання академічної доброчесності
Основні категорії інформації, що обробляється	Навчально-методичні матеріали, випускні роботи здобувачів освіти
Адміністрування або відповідальна особа з боку Коледжу	Адміністратор програмного комплексу StrikePlagiarism
Спосіб доступу та автентифікації	Обліковий запис адміністратора та засоби автентифікації

ДОДАТОК 2. МІНІМАЛЬНІ ВИМОГИ ДО ПАРОЛІВ ТА ЗАХИСТУ ОБЛІКОВИХ ЗАПИСІВ

Дотримання цих Мінімальних вимог є обов'язковим для осіб, які використовують інформаційні ресурси та облікові записи Коледжу. Вимоги переглядаються у разі зміни законодавства України, рекомендацій компетентних державних органів, суттєвої зміни інформаційної інфраструктури Коледжу або виявлення недостатності встановлених заходів захисту.

1. Загальні вимоги

1.1. Ці Мінімальні вимоги визначають основні правила створення, використання та захисту паролів і облікових записів працівників та здобувачів освіти під час використання інформаційних ресурсів, систем, електронних сервісів і технічних засобів Коледжу.

1.2. Вимоги застосовуються в межах технічних можливостей відповідної інформаційної системи та з урахуванням установлених її власником, розпорядником або адміністратором правил автентифікації.

1.3. Якщо правила відповідної інформаційної системи встановлюють більш суворі вимоги до паролів або автентифікації, застосовуються вимоги такої системи.

2. Вимоги до створення паролів

2.1. Пароль повинен:

- містити не менше 8 символів, якщо відповідна інформаційна система підтримує використання паролів такої довжини;
- бути складним для вгадування та не містити очевидної інформації про користувача;
- відрізнятися від паролів, що використовуються користувачем для особистих облікових записів;
- бути унікальним для інформаційних ресурсів, що мають істотне значення для діяльності Коледжу або забезпечують доступ до інформації з обмеженим доступом.

2.2. Рекомендується використовувати довгі парольні фрази або комбінації слів, символів і цифр, які легко запам'ятати користувачу, але складно підібрати іншій особі.

2.3. Не допускається використання як паролів:

- імені, прізвища, логіна користувача або їх очевидних комбінацій;
- дати народження, номера телефону та інших загальнодоступних персональних відомостей, простих послідовностей символів, цифр або клавіш клавіатури;
- стандартних паролів, установлених виробником обладнання чи програмного забезпечення;
- одного й того самого пароля для службових і особистих облікових записів.

3. Використання та зберігання паролів

3.1. Паролі є персональними засобами автентифікації та не підлягають передаванню іншим особам.

3.2. Користувачі зобов'язані вживати заходів для запобігання розголошенню, втраті або компрометації паролів.

3.3. Не допускається:

- повідомляти пароль іншим особам, у тому числі керівникам, колегам, адміністраторам інформаційних систем або працівникам технічної підтримки;
- надсилати паролі електронною поштою, через месенджери або інші незахищені канали зв'язку;
- зберігати паролі у відкритому вигляді у текстових файлах, електронних таблицях, веббраузерах або інших доступних стороннім особам місцях;
- залишати записи з паролями біля робочого місця або разом із технічним засобом, для доступу до якого вони використовуються.

3.4. Для створення та зберігання унікальних паролів допускається використання надійних менеджерів паролів з урахуванням установлених у Коледжі вимог безпеки.

4. Зміна паролів

4.1. Обов'язкова періодична зміна пароля без наявності ознак або обґрунтованої підозри щодо його компрометації не вимагається, якщо інше не встановлено законодавством України або правилами відповідної інформаційної системи.

4.2. Пароль підлягає невідкладній зміні у разі:

- виявлення або обґрунтованої підозри щодо його компрометації;
- отримання відомостей про несанкціонований доступ до облікового запису;
- використання пароля на інформаційному ресурсі, щодо якого стало відомо про витік облікових даних;
- повідомлення пароля іншій особі або його випадкового розголошення;

- отримання відповідної вимоги адміністратора інформаційної системи або відповідальної особи у зв’язку з виявленою загрозою безпеці.

4.3. Тимчасові та початкові паролі, надані користувачу адміністратором інформаційної системи, повинні бути змінені під час першого входу, якщо це підтримується відповідною системою.

5. Багатофакторна автентифікація

5.1. Багатофакторна автентифікація використовується для захисту облікових записів у випадках, передбачених законодавством, вимогами відповідної інформаційної системи або локальними нормативними актами Коледжу.

5.2. Коди підтвердження, резервні коди та інші додаткові засоби автентифікації не повинні передаватися іншим особам.

6. Захист облікових записів

6.1. Користувач зобов’язаний використовувати лише облікові записи, надані йому у встановленому порядку.

6.2. Використання облікового запису іншого користувача або надання власного облікового запису іншій особі не допускається.

6.3. Користувач повинен завершувати робочий сеанс або блокувати технічний засіб у разі залишення робочого місця без нагляду.

6.4. У разі отримання повідомлення про спробу входу, запиту на підтвердження автентифікації або зміну пароля, які користувач не ініціював, він повинен відхилити такий запит, за можливості змінити пароль та повідомити відповідальну особу або адміністратора відповідної системи.

7. Обов’язки адміністраторів інформаційних ресурсів

7.1. Адміністратори інформаційних ресурсів у межах наданих повноважень та технічних можливостей відповідних систем:

- забезпечують зміну стандартних паролів, установлених виробником програмного забезпечення або обладнання;
- не здійснюють зберігання паролів користувачів у відкритому вигляді;
- застосовують доступні механізми захисту адміністративних облікових записів;
- забезпечують блокування або припинення доступу до облікових записів у випадках, передбачених Положенням;
- інформують відповідальну особу про виявлені випадки компрометації облікових записів або інші істотні порушення вимог безпеки.

ДОДАТОК 3.
ПРАВИЛА ВИКОРИСТАННЯ ЗМІННИХ НОСІЇВ ІНФОРМАЦІЇ

1. Загальні положення

1.1. Ці Правила визначають основні вимоги до використання змінних носіїв інформації під час роботи з інформаційними ресурсами та технічними засобами Коледжу.

1.2. До змінних носіїв інформації у цих Правилах належать USB-флешнакопичувачі, зовнішні жорсткі диски та твердотільні накопичувачі, карти пам’яті, оптичні диски та інші переносні носії, призначені для запису, зберігання або перенесення інформації. Засоби зберігання особистих ключів КЕП використовуються відповідно до законодавства України у сфері електронної ідентифікації та електронних довірчих послуг, вимог надавачів електронних довірчих послуг і Положення.

1.3. Змінні носії використовуються лише за наявності службової, освітньої або іншої правомірної необхідності. Під час використання змінних носіїв повинні вживатися заходи, спрямовані на запобігання зараженню технічних засобів шкідливим програмним забезпеченням, втраті носіїв, несанкціонованому доступу до інформації, її неправомірному копіюванню, зміні або поширенню.

2. Використання змінних носіїв

2.1. До технічних засобів Коледжу допускається підключення змінних носіїв, необхідних для виконання посадових, службових або освітніх завдань. Використання носіїв невідомого походження або носіїв, щодо безпеки яких є обґрунтовані сумніви, не допускається.

2.2. Перед відкриттям або копіюванням файлів зі змінного носія він повинен бути перевірений доступними засобами захисту від шкідливого програмного забезпечення. У разі виявлення шкідливого програмного забезпечення, підозрілих файлів або інших ознак загрози користувач припиняє роботу з носієм та повідомляє відповідальну особу.

2.3. Не допускається використання змінних носіїв для:

- перенесення або зберігання програмного забезпечення, файлів чи іншої інформації, використання яких суперечить законодавству України або встановленим у Коледжі вимогам;
- несанкціонованого копіювання інформації з інформаційних ресурсів Коледжу;
- обходу встановлених засобів захисту та обмежень доступу;
- постійного зберігання єдиного примірника службової інформації, необхідної для діяльності Коледжу.

2.4. На змінний носій повинна копіюватися лише інформація, необхідна для виконання відповідного завдання. Після припинення необхідності у зберіганні інформації на носії вона підлягає видаленню з урахуванням установлених вимог до строків зберігання документів та інформації.

3. Захист інформації на змінних носіях

3.1. Зберігання на змінних носіях персональних даних, службової інформації та іншої інформації з обмеженим доступом допускається лише за наявності правомірної необхідності та за умови застосування заходів захисту, що відповідають характеру інформації та можливим ризикам.

3.2. Для захисту інформації з обмеженим доступом на змінних носіях за необхідності застосовуються шифрування, захист паролем або інші доступні засоби захисту, якщо їх використання відповідає вимогам законодавства щодо відповідної категорії інформації.

3.3. Не допускається залишати змінні носії, на яких зберігається інформація з обмеженим доступом, без нагляду у місцях, доступних стороннім особам. Такі носії після завершення роботи зберігаються у приміщеннях, шафах, сейфах або інших місцях, що забезпечують обмеження неконтрольованого доступу.

3.4. Передавання змінного носія іншому працівнику допускається лише за наявності службової необхідності та за умови, що одержувач має право на доступ до інформації, яка зберігається на носії.

4. Використання особистих змінних носіїв

4.1. Використання особистих змінних носіїв працівників на технічних засобах Коледжу допускається лише за наявності обґрунтованої необхідності та з дотриманням вимог цих Правил.

4.2. Зберігання інформації з обмеженим доступом на особистих змінних носіях допускається лише у випадках, коли таке використання обумовлено службовою необхідністю із застосуванням належних заходів захисту.

4.3. Відповідальна особа має право вимагати припинення використання змінного носія, якщо його використання створює загрозу безпеці інформації або технічним засобам Коледжу.

5. Втрата, пошкодження або компрометація носія

5.1. У разі втрати, викрадення, пошкодження змінного носія або виникнення підозри щодо несанкціонованого доступу до інформації, що на ньому зберігається, працівник зобов’язаний невідкладно повідомити відповідальну особу та свого безпосереднього керівника.

5.2. Відповідальна особа оцінює можливі наслідки події та за необхідності організовує вжиття заходів відповідно до порядку реагування на кіберінциденти, встановленого цим Положенням.

6. Припинення використання змінних носіїв

6.1. Перед передаванням змінного носія іншому користувачу, повторним використанням для іншої мети, списанням, ремонтом, поверненням власнику або утилізацією інформація, що не підлягає подальшому зберіганню, повинна бути видалена.

6.2. Якщо на носії зберігалася інформація з обмеженим доступом або інша інформація, несанкціоноване відновлення якої може завдати шкоди, застосовується спосіб очищення або знищення носія, що мінімізує можливість відновлення такої інформації.

7. Прикінцеві положення

7.1. Користувачі змінних носіїв несуть відповідальність за дотримання цих Правил у межах, установлених законодавством України та Положенням.

7.2. Контроль за дотриманням цих Правил здійснюється відповідальною особою, керівниками структурних підрозділів та іншими уповноваженими особами в межах їх повноважень.

7.3. Питання використання змінних носіїв, не врегульовані цими Правилами, вирішуються відповідно до цього Положення, законодавства України та вимог відповідної інформаційної системи.

ДОДАТОК 4. ПОРЯДОК РЕЗЕРВНОГО КОПІЮВАННЯ ТА ВІДНОВЛЕННЯ ІНФОРМАЦІЇ

1. Загальні положення

1.1. Цей Порядок визначає основні вимоги до організації резервного копіювання, зберігання резервних копій та відновлення інформації, що використовується у діяльності Коледжу.

1.2. Резервне копіювання здійснюється з метою забезпечення можливості відновлення інформації у разі її втрати, пошкодження, знищення, неправомірної зміни, технічної несправності, дії шкідливого програмного забезпечення, кіберінциденту або інших подій, що призвели до порушення доступності чи цілісності інформації.

1.3. Вимоги цього Порядку застосовуються до інформації, резервне копіювання якої належить до повноважень і технічних можливостей Коледжу.

1.4. Резервне копіювання інформації, що зберігається та обробляється у зовнішніх інформаційних системах і сервісах, здійснюється Коледжем лише у випадках, коли відповідна функціональна можливість надана користувачу системи та існує необхідність створення додаткової копії інформації.

2. Організація резервного копіювання

2.1. Резервному копіюванню підлягає інформація, втрата, пошкодження або тривала недоступність якої може істотно вплинути на діяльність Коледжу.

2.2. Необхідність резервного копіювання конкретної інформації визначається з урахуванням:

- значущості інформації для діяльності Коледжу;
- можливих наслідків її втрати, пошкодження або недоступності;
- частоти внесення змін до інформації;
- можливості відновлення інформації з інших джерел;
- строків зберігання відповідних документів та інформації;
- наявних технічних можливостей і вимог до захисту інформації.

2.3. Визначення інформації, що підлягає резервному копіюванню та саме резервне копіювання здійснюється керівниками структурних підрозділів та працівниками, відповідальними за використання відповідних інформаційних ресурсів.

3. Створення та зберігання резервних копій

3.1. Періодичність резервного копіювання визначається залежно від значущості інформації та частоти її зміни. Резервні копії повинні створюватися з такою періодичністю, щоб можлива втрата інформації за

період між останнім резервним копіюванням та подією, що спричинила необхідність відновлення, не призводила до неприйнятних наслідків для діяльності Коледжу.

3.2. Резервні копії мають зберігатися окремо від основної інформації у спосіб, що зменшує ризик їх одночасної втрати, пошкодження або знищення внаслідок технічної несправності, шкідливого програмного забезпечення, кіберінциденту чи іншої несприятливої події.

3.3. Для зберігання резервних копій можуть використовуватися зовнішні накопичувачі, окремі технічні засоби, мережеві сховища, хмарні сервіси або інші засоби, використання яких відповідає законодавству України та встановленим у Коледжі вимогам захисту інформації.

3.4. Резервні копії повинні бути захищені від несанкціонованого доступу, неправомірної зміни та видалення. Якщо резервні копії містять персональні дані, службову інформацію або іншу інформацію з обмеженим доступом, до них застосовуються заходи захисту, що відповідають правовому режиму та характеру такої інформації.

3.5. Доступ до резервних копій надається лише працівникам, яким він необхідний для виконання посадових обов’язків, створення резервних копій, перевірки їх стану або відновлення інформації.

4. Перевірка резервних копій та відновлення інформації

4.1. Стан резервних копій та можливість відновлення інформації підлягають періодичній перевірці. Періодичність та обсяг перевірки визначаються з урахуванням значущості інформації, способу створення резервних копій та наявних технічних можливостей.

4.2. У разі виявлення пошкодження резервної копії, неможливості відновлення інформації або інших недоліків, відповідальна особа та працівник, відповідальний за відповідний інформаційний ресурс, вживають у межах своїх повноважень заходів щодо усунення виявлених недоліків.

4.3. Відновлення інформації з резервної копії здійснюється у разі втрати, пошкодження, неправомірної зміни, недоступності основної інформації або в інших випадках, коли відновлення необхідне для забезпечення належної діяльності Коледжу.

4.4. Перед відновленням інформації за можливості встановлюються причини її втрати, пошкодження або недоступності та вживаються заходи для запобігання повторному пошкодженню чи втраті відновленої інформації. Якщо необхідність відновлення пов’язана з кіберінцидентом, відповідні дії здійснюються з урахуванням установленого цим Положенням порядку реагування на кіберінциденти.

5. Строки зберігання та видалення резервних копій

5.1. Строки зберігання резервних копій визначаються з урахуванням:

- призначення та значущості інформації;
- періодичності створення резервних копій;
- наявних технічних ресурсів;
- необхідності збереження декількох попередніх версій інформації.

5.2. Резервні копії, потреба у зберіганні яких припинилася, видаляються або знищуються у спосіб, що враховує характер інформації та мінімізує ризик її несанкціонованого відновлення.

6. Обов’язки та контроль

6.1. Працівники, відповідальні за створення та зберігання резервних копій:

- забезпечують виконання резервного копіювання відповідно до визначеної періодичності;
- забезпечують належне зберігання резервних копій та обмеження доступу до них;
- повідомляють відповідальну особу про виявлені проблеми, що можуть призвести до неможливості створення резервних копій або відновлення інформації.

6.2. Відповідальна особа координує організацію резервного копіювання та проведення перевірок можливості відновлення інформації.

6.3. Контроль за виконанням цього Порядку здійснюється відповідальною особою та керівниками структурних підрозділів у межах їх повноважень.

ДОДАТОК 5.
ПОРЯДОК ПОВІДОМЛЕННЯ ПРО КІБЕРІНЦИДЕНТИ

1. Загальні положення

1.1. Цей Порядок визначає основні вимоги до повідомлення про виявлені або ймовірні кіберінциденти та інші події, що можуть створювати загрозу безпеці інформації, інформаційним ресурсам або технічним засобам Коледжу.

1.2. Метою повідомлення про кіберінциденти є забезпечення своєчасного отримання інформації, необхідної для оцінювання події, вжиття заходів реагування, обмеження можливих негативних наслідків та організації взаємодії з відповідними суб'єктами.

1.3. Повідомленню підлягають події, що мають ознаки кіберінциденту або обґрунтовано можуть свідчити про загрозу безпеці інформації чи інформаційних ресурсів Коледжу.

2. Особи, зобов'язані повідомляти про кіберінциденти

2.1. Працівники та здобувачі освіти Коледжу, яким надано доступ до інформаційних ресурсів або технічних засобів Коледжу, зобов'язані повідомляти про виявлені ними ознаки кіберінцидентів відповідно до цього Порядку.

2.2. Повідомленню підлягають, зокрема:

- підозра щодо несанкціонованого доступу до облікового запису, інформації, інформаційного ресурсу або технічного засобу;
- втрата, викрадення або ймовірна компрометація пароля, засобу багатофакторної автентифікації, КЕП, носія інформації чи технічного засобу, на якому оброблялася інформація Коледжу;
- виявлення шкідливого програмного забезпечення або ознак зараження технічного засобу;
- отримання підозрілих електронних повідомлень, відкриття шкідливого вкладення, перехід за підозрілим посиланням або введення облікових даних на ймовірно шахрайському ресурсі;
- незрозуміла або неочікувана зміна, видалення, блокування чи недоступність інформації;
- порушення роботи інформаційного ресурсу, яке може бути пов'язане з кібератакою або іншими неправомірними діями;
- неправомірне розголошення, передавання або надання доступу до інформації з обмеженим доступом;
- інші підозрілі події, які можуть створювати загрозу безпеці інформації або інформаційних ресурсів Коледжу.

3. Порядок внутрішнього повідомлення

3.1. Особа, яка виявила ознаки кіберінциденту, повідомляє про них невідкладно після виявлення події:

- відповідальну особу за технічний захист інформації та кібербезпеку;
- адміністратора відповідного інформаційного ресурсу, якщо повідомити відповідальну особу безпосередньо неможливо.

3.2. Особа, яка отримала повідомлення про можливий кіберінцидент відповідно до підпункту 2 пункту 3.1 цього Порядку, забезпечує його невідкладне передавання відповідальній особі.

4. Зміст повідомлення

4.1. Повідомлення про кіберінцидент за можливості повинно містити:

- прізвище, ім’я та посаду або статус особи, яка повідомляє про подію;
- дату і приблизний час виявлення події;
- інформаційний ресурс, обліковий запис, технічний засіб або інформацію, яких стосується подія;
- короткий опис виявлених ознак та обставин події;
- відомості про дії, здійснені особою до моменту повідомлення;
- інформацію про можливе поширення події на інші технічні засоби або інформаційні ресурси, якщо така інформація відома;
- контактні дані для уточнення обставин події.

4.2. До повідомлення за можливості додаються знімки екрана, електронні повідомлення, назви файлів, час виникнення помилок та інші доступні матеріали, які можуть сприяти встановленню обставин події.

5. Дії особи, яка виявила кіберінцидент

5.1. До отримання вказівок відповідальної особи або адміністратора відповідного інформаційного ресурсу особа, яка виявила кіберінцидент, повинна:

- припинити дії, що можуть сприяти подальшому поширенню загрози або збільшенню негативних наслідків;
- не видаляти підозрілі файли, електронні повідомлення, журнали подій та інші відомості, що можуть мати значення для встановлення обставин інциденту;
- не здійснювати самостійне переустановлення операційної системи, очищення технічного засобу або інші дії, що можуть призвести до втрати відомостей про інцидент;
- не поширювати інформацію про інцидент серед сторонніх осіб, якщо таке поширення не передбачене законодавством або службовою необхідністю;

- виконувати вказівки відповідальної особи та інших уповноважених осіб щодо локалізації інциденту та збереження необхідної інформації.

5.2. Якщо продовження роботи з технічним засобом може призвести до поширення шкідливого програмного забезпечення, несанкціонованого передавання інформації або інших істотних негативних наслідків, користувач припиняє роботу з відповідним технічним засобом та, за можливості, відключає його від мережевих з'єднань без вимкнення живлення, якщо інші дії не визначені відповідальною особою.

6. Отримання та опрацювання повідомлення

6.1. Відповідальна особа після отримання повідомлення:

- уточнює за необхідності обставини події;
- здійснює первинне оцінювання отриманої інформації;
- визначає необхідність вжиття невідкладних заходів;
- організовує реєстрацію кіберінциденту у випадках, передбачених Положенням;
- інформує керівника Коледжу про істотні кіберінциденти;
- забезпечує подальші дії відповідно до цього Положення.

7. Зовнішнє повідомлення про кіберінциденти

7.1. Повідомлення компетентних державних органів, власників, розпорядників або адміністраторів інформаційних систем та інших суб'єктів здійснюється у випадках та порядку, передбачених законодавством України, правилами відповідної інформаційної системи, договорами та іншими обов'язковими для Коледжу вимогами.

7.2. Зовнішнє повідомлення про кіберінцидент здійснюється керівником Коледжу, відповідальною особою або іншою уповноваженою особою в межах наданих повноважень.

ДОДАТОК 6. ЖУРНАЛ РЕЄСТРАЦІЇ КІБЕРІНЦИДЕНТІВ

6.1. Форма ведення журналу:

№ з/п	Дата і час виявлення	Інформаційний ресурс / технічний засіб	Короткий опис кіберінциденту	Вжиті заходи	Наслідки та результат усунення	Дата завершення реагування	Примітки

6.2. Журнал ведеться відповідальною особою за технічний захист інформації та кібербезпеку в електронній та/або паперовій формі.

6.3. До Журналу вносяться відомості про істотні кіберінциденти відповідно до цього Положення. Записи здійснюються на підставі наявної та перевіреної інформації та за необхідності доповнюються в процесі реагування на кіберінцидент.

6.4. Доступ до Журналу надається лише особам, яким відповідні відомості необхідні для виконання посадових обов’язків або здійснення повноважень, установлених законодавством України.

ДОДАТОК 7. БАЗОВІ ПРАВИЛА КІБЕРГІГІЄНИ ДЛЯ ПРАЦІВНИКІВ І ЗДОБУВАЧІВ ОСВІТИ

1. Загальні положення

1.1. Ці Правила визначають основні вимоги кібергігієни, яких повинні дотримуватися працівники та здобувачі освіти Коледжу під час використання інформаційних ресурсів, електронних сервісів, облікових записів і технічних засобів Коледжу.

1.2. Користувачі інформаційних ресурсів повинні дотримуватися вимог цих Правил, цього Положення, інших локальних нормативних актів Коледжу та правил використання відповідних інформаційних систем і сервісів.

2. Захист облікових записів

2.1. Користувачі зобов'язані:

- використовувати надійні паролі та не передавати їх іншим особам;
- не використовувати службові паролі для особистих облікових записів;
- використовувати багатофакторну автентифікацію у випадках, передбачених вимогами відповідної інформаційної системи або Коледжу;
- не повідомляти іншим особам коди підтвердження входу, резервні коди та інші засоби автентифікації;
- невідкладно повідомляти відповідальну особу або адміністратора відповідного інформаційного ресурсу про підозру щодо компрометації облікового запису.

3. Безпечне використання електронної пошти та мережі Інтернет

3.1. Користувачі повинні критично оцінювати електронні повідомлення, посилання, вкладення та запити щодо надання персональних, облікових або платіжних даних.

3.2. Не допускається:

- відкривати вкладення та переходити за посиланнями у підозрілих повідомленнях;
- вводити облікові дані на вебресурсах, справжність яких викликає обґрунтовані сумніви;
- передавати паролі, коди підтвердження та інші засоби автентифікації у відповідь на запити, отримані електронною поштою, через месенджери або телефонні дзвінки;
- використовувати інформаційні ресурси Коледжу для поширення шкідливого програмного забезпечення, шахрайських повідомлень або здійснення інших неправомірних дій.

3.3. У разі отримання підозрілого повідомлення користувач повинен утриматися від взаємодії з його вмістом та за необхідності повідомити відповідальну особу або адміністратора відповідного інформаційного ресурсу.

4. Безпечне використання технічних засобів і програмного забезпечення

4.1. Користувачі зобов'язані:

- використовувати технічні засоби та програмне забезпечення відповідно до їх призначення і наданих повноважень;
- блокувати робочий сеанс у разі залишення технічного засобу без нагляду;
- не встановлювати без належного дозволу програмне забезпечення на технічні засоби Коледжу;
- не відключати та не змінювати налаштування засобів захисту інформації без відповідних повноважень;
- не підключати до технічних засобів Коледжу носії та пристрої невідомого походження;
- повідомляти про виявлені несправності, підозрілу поведінку програмного забезпечення та інші ознаки можливого порушення безпеки.

5. Захист інформації

5.1. Користувачі повинні:

- отримувати доступ лише до інформації, необхідної для виконання посадових, службових, освітніх або інших правомірних завдань;
- не передавати інформацію з обмеженим доступом особам, які не мають права на її отримання;
- не зберігати інформацію з обмеженим доступом на особистих пристроях, носіях або в особистих хмарних сховищах без правомірної необхідності та належних заходів захисту;
- не залишати без нагляду документи, технічні засоби та носії інформації, якщо це може призвести до несанкціонованого доступу до інформації;
- дотримуватися встановлених у Коледжі правил використання змінних носіїв інформації та засобів КЕП.

6. Дії у разі підозрілої події або кіберінциденту

6.1. Користувач повинен невідкладно повідомити відповідальну особу або адміністратора відповідного інформаційного ресурсу в разі:

- підозри щодо несанкціонованого доступу до облікового запису або інформації;
- втрати або ймовірної компрометації пароля, засобу автентифікації, КЕП, технічного засобу чи носія інформації;
- виявлення шкідливого програмного забезпечення;

- відкриття підозрілого вкладення, переходу за ймовірно шкідливим посиланням або введення облікових даних на підозрілому вебресурсі;
- виявлення інших обставин, які можуть свідчити про кіберінцидент.

6.2. Повідомлення про можливий кіберінцидент здійснюється відповідно до Порядку повідомлення про кіберінциденти, установленого Додатком 5 до цього Положення.

7. Підвищення обізнаності з питань кібербезпеки

7.1. Працівники та здобувачі освіти повинні ознайомлюватися з інформаційними матеріалами, рекомендаціями та попередженнями щодо актуальних кіберзагроз, які доводяться до їх відома Коледжем.

7.2. Працівники, які використовують інформаційні ресурси Коледжу, проходять передбачені Коледжем інформаційні, навчальні та інструктивні заходи з питань кібергігієни та кібербезпеки.

7.3. Інформаційні та навчальні заходи для здобувачів освіти проводяться з урахуванням характеру інформаційних ресурсів, які вони використовують, актуальних кіберзагроз та організації освітнього процесу.

7.4. Дотримання цих Правил є обов’язковим для працівників і здобувачів освіти під час використання інформаційних ресурсів та технічних засобів Коледжу.

7.5. Особи, які порушили вимоги цих Правил, несуть відповідальність у випадках та порядку, встановлених законодавством України, цим Положенням та іншими локальними нормативними актами Коледжу.