

**ПРИВАТНИЙ ПІСЛЯДИПЛОМНИЙ ЗАКЛАД ОСВІТИ
«ІНСТИТУТ ПРОФЕСІЙНИХ ТРАНСФОРМАЦІЙ»**

**ЗАГАЛЬНА КОРОТКОСТРОКОВА ПРОГРАМА ПІДВИЩЕННЯ
КВАЛІФІКАЦІЇ**

«Інформаційна безпека та захист персональних даних»

Шифр програми: ЗК/2024/007

Рік запровадження програми: 2024

Програму затверджено: наказом директора Приватного післядипломного закладу освіти «Інститут професійний трансформацій»

(наказ від 08 липня 2024 р. № 06-3)

Програму погоджено наказом НАДС: наказ №129-24 від 29.08.2024 р.

ПРОФІЛЬ ПРОГРАМИ

1. Загальна інформація

| | |
|---|--|
| Назва програми | Інформаційна безпека та захист персональних даних |
| Шифр програми | ЗК/2024/007 |
| Тип програми за змістом | загальна |
| Форма навчання | дистанційна |
| Цільова група | державні службовці, які займають посади державної служби категорії «Б» та «В» |
| Передумови навчання за програмою | проходження онлайн курсу (доступно на сайті у розділі Підвищення кваліфікації: https://www.ipt.cn.ua/sertyfikatni-prohramy/ з отриманням відповідного сертифіката |
| Найменування замовника освітніх послуг у сфері професійного навчання за програмою | - |
| Найменування партнера (партнерів) програми | - |
| Обсяг програми | 1 кредит ЄКТС |
| Тривалість програми та організація навчання | тривалість програми становить 5 днів з урахуванням запланованих годин для дистанційних занять |
| Мова(и) викладання | державна |
| Напрям(и) підвищення кваліфікації, який(які) охоплює програма | цифрова грамотність |
| Перелік професійних компетентностей, на підвищення рівня яких спрямовано програму | вміння використовувати комп'ютерне обладнання та програмне забезпечення, використовувати офісну техніку |
| Укладач(і) програми | Шестаковська Тетяна Леонідівна, доктор наук з державного управління, доцент, ректор Чернігівського інституту інформації, бізнесу і права ЗВО «МНТУ» Shestakovska27@gmail.com |

2. Загальна мета

Ознайомити слухачів із засадами державної інформаційної політики та сформувані в них відповідні знання й навички з питань захисту персональних даних, програмного забезпечення та інформаційної безпеки.

3. Очікувані результати навчання

| | |
|--|--|
| За результатами навчання учасники професійного навчання повинні демонструвати: | |
| Знання | основних положень вітчизняного законодавства в сфері інформаційної безпеки, публічної інформації та захисту персональних даних; загроз та небезпек, які можуть виникати при роботі з інформацією; організаційних засад збереження та захисту персональних даних. |
| Уміння | керуватися законодавством України з питань інформаційної безпеки, публічної інформації та захисту персональних даних під час здійснення своєї службової діяльності; здійснювати оцінку потенційних загроз, які можуть виникати при роботі з інформацією; вживати заходів в рамках своїх посадових компетенцій щодо збереження та захисту персональних даних. |
| Навички | дотримуватись норм інформаційної безпеки даних. |

4. Викладання та навчання

| (методи навчання, форми проведення навчальних занять) | |
|--|--|
| Навчання здійснюється у формі синхронних дистанційних занять та самостійного опрацювання частини навчального матеріалу. У процесі викладання діяльність викладача спрямована на розробку і використання ефективних форм, змісту, методів, прийомів і засобів навчання, які сприяють підвищенню інтересу, самостійності, творчої активності слухачів у засвоєнні знань, набутті вмінь і навичок, їх практичному застосуванні, а також у прийнятті самостійних рішень: мозковий штурм; проблемні лекції та семінари; тематичні дискусії; ділові ігри; метод конкретних ситуацій. | |
| 5. Ресурсне забезпечення дистанційного навчання | |
| Назви вебплатформи, вебсайту, електронної системи навчання, через які здійснюватиметься таке навчання, посилання (вебадреса) | дистанційне навчання в синхронному режимі — доступ до вебкабінету відеоконференції надається під час реєстрації |
| Назва дистанційного курсу (модуля) | - |
| 6. Оцінювання і форми поточного, підсумкового контролю | |
| Складові оцінювання та їх питома вага у підсумковій оцінці (%) | відвідування занять дистанційно – 10%; поточний контроль – 60%; підсумковий контроль – 30%; Документ про підвищення кваліфікації видається за умови набрання учасником професійного навчання не менше ніж 75%, що обраховані з урахуванням питомої ваги кожного із критеріїв оцінювання |
| Форма та періодичність поточного контролю | поточний контроль проводиться шляхом спілкування зі слухачами під час занять, обговорення практичних ситуацій, розв'язання ситуаційних завдань, а також перевірки виконання тестових завдань |
| Форма підсумкового контролю | Тестування |

СТРУКТУРА ПРОГРАМИ

| <i>Назва теми</i> | <i>Кількість годин</i> | | | | |
|--|--|--------------------------|----------------------------|-------------------------|-----------------------------------|
| | <i>загальна кількість годин/ кредитів ЄКТС</i> | <i>у тому числі:</i> | | | |
| | | <i>Аудиторні заняття</i> | <i>дистанційні заняття</i> | <i>Навчальні візити</i> | <i>самостійна робота слухачів</i> |
| 1 | 2 | 3 | 4 | 5 | 6 |
| Тема 1. Інформаційна безпека в системі національної безпеки України | 6 | - | 5 | - | 1 |
| Тема 2. Загрози, що виникають під час роботи з інформацією та персональними даними в сучасному кіберпросторі | 6 | - | 5 | - | 1 |
| Тема 3. Вітчизняний та зарубіжний досвід розповсюдження та оприлюднення публічної інформації та захисту персональних даних | 6 | - | 5 | - | 1 |
| Тема 4. Особливості захисту персональних даних в сучасному кіберпросторі | 5 | - | 4 | - | 1 |
| Тема 5. Використання штучного інтелекту в роботі державного службовця: переваги та ризики | 5 | - | 4 | - | 1 |
| Підсумковий контроль результатів навчання | 2 | - | 2 | - | |
| РАЗОМ | 30/1 | - | 25 | - | 5 |

ЗМІСТ ПРОГРАМИ

Тема 1. Інформаційна безпека в системі національної безпеки України.

Перелік питань для вивчення теми

Значення інформаційної безпеки для національної безпеки України. Правові основи забезпечення інформаційної безпеки в Україні. Основні загрози інформаційній безпеці України. Системи захисту інформації. Кібербезпека як ключовий елемент інформаційної безпеки. Розвиток національної інфраструктури інформаційної безпеки. Психологічні аспекти інформаційної безпеки. Перспективи розвитку інформаційної безпеки в Україні.

Форма проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми

Форма проведення – лекція-демонстрація, семінар-практикум. Методи навчання – бесіда, візуалізація, мозковий штурм, метод мікрофон.

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання

Роль приватного сектору у забезпеченні інформаційної безпеки.

Тема 2. Загрози, що виникають під час роботи з інформацією та персональними даними в сучасному кіберпросторі.

Перелік питань для вивчення теми

Кіберзлочинність. Кібершпигунство. Порушення конфіденційності даних. Несанкціонований доступ. Вразливості в програмному забезпеченні. Загрози, пов'язані з хмарними технологіями. Інсайдерські загрози. Загрози, пов'язані з інтернетом речей (IoT). Мобільні загрози. Загрози, пов'язані з соціальними мережами.

Форма проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми.

Форма проведення – лекція-демонстрація. Методи навчання – бесіда, візуалізація.

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання

Захист від загроз.

Тема 3. Вітчизняний та зарубіжний досвід розповсюдження та оприлюднення публічної інформації та захисту персональних даних.

Перелік питань для вивчення теми

Законодавче регулювання та інституційні механізми. Платформи для оприлюднення інформації. Загальний регламент захисту даних (GDPR). Платформи відкритих даних. Закон про свободу інформації (FOIA). Високі стандарти захисту персональних даних, особливо в країнах ЄС з їх GDPR. Активний розвиток платформ відкритих даних, що підвищує прозорість та підзвітність урядів. Сучасне законодавство, що враховує нові технологічні виклики. Необхідність адаптації міжнародного досвіду до національних умов. Підвищення рівня цифрової грамотності населення. Вдосконалення законодавчої бази та механізмів контролю за дотриманням законів.

Форма проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми

Форма проведення – лекція-демонстрація. Методи навчання – демонстрація, лекція-бесіда, метод залучення.

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання

Підвищення обізнаності громадян про права на доступ до інформації та захист персональних даних.

Тема 4. Особливості захисту персональних даних в сучасному кіберпросторі.

Перелік питань для вивчення теми

Загальний регламент захисту даних (GDPR) в Європейському Союзі. Закони США про захист персональних даних. Закон України "Про захист персональних даних". Шифрування даних. Аутентифікація та авторизація. Використання фаєрволів для контролю доступу до мережі. Системи виявлення та запобігання вторгнень (IDS/IPS). Управління правами доступу до даних та ресурсів. Використання політик безпеки для контролю доступу до конфіденційної інформації. Постійний моніторинг систем безпеки для виявлення аномалій та потенційних загроз. Розробка процедур для швидкого реагування на порушення безпеки даних. Впровадження стандартів ISO/IEC 27001 для управління інформаційною безпекою.

Форма проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми

Форма проведення – лекція-демонстрація, семінар-тренінг. Методи навчання – лекція-бесіда, метод мікрофон, мозковий штурм.

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання

Обмін інформацією про загрози та методи захисту.

Тема 5. Використання штучного інтелекту в роботі державного службовця: переваги та ризики.

Перелік питань для вивчення теми

Вплив штучного інтелекту на підвищення ефективності державного управління. Покращення якості надання державних послуг за допомогою ШІ. Проблеми конфіденційності та захисту даних при використанні ШІ в державному секторі. Етичні аспекти використання ШІ у державному управлінні. Роль штучного інтелекту в прийнятті рішень державними службовцями. Соціальні та економічні наслідки впровадження ШІ у державному секторі. Міжнародний досвід використання ШІ у державному управлінні. Розвиток нормативно-правової бази для використання ШІ у державному секторі. Навчання та підготовка державних службовців до роботи з ШІ.

Форма проведення навчальних занять та методи навчання, які дозволяють розкрити зміст теми

Форма проведення – лекція-демонстрація. Методи навчання – лекція-бесіда.

Перелік питань, які виносяться на самостійну роботу учасників професійного навчання

Використання ШІ для забезпечення громадської безпеки та правопорядку.

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Оцінювання результатів навчання за загальною короткостроковою програмою підвищення кваліфікації здійснюється шляхом поточного та підсумкового контролю.

Поточний контроль проводиться шляхом спілкування зі слухачами під час занять, відбувається обговорення практичних ситуацій, розв'язання ситуаційних завдань, а також перевірки виконання тестових завдань. Підсумковий контроль здійснюється шляхом тестування через платформу Google Meet.

Оцінювання результатів навчання здійснюється за такими складовими:

дистанційних (в синхронному режимі) занять та активна участь під час таких занять (виступи, рефлексія, робота в парах, відповіді на запитання, швидке опитування тощо) – 10 %;

поточний контроль – 60 %;

підсумковий контроль – 30 %.

Підсумкова оцінка складається із суми всіх оцінок за кожною складовою оцінювання результатів навчання. Учасник професійного навчання отримує документ про підвищення кваліфікації, якщо набрав не менше 75 % від загального значення підсумкової оцінки.

ЛІТЕРАТУРА, ІНФОРМАЦІЙНІ РЕСУРСИ, ОБОВ'ЯЗКОВІ ДЛЯ ОПРАЦЮВАННЯ.

1. Панченко О. А. Інформаційна безпека в епоху турбулентності: державно-управлінський аспект: монографія. Київ: КВІЦ, 2020. 331 с.
2. Ніколаєнко Н. О., Комарчук О. О. Засоби масової комунікації як детермінанти гібридної війни: монографія / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв: НУК, 2021. 217 с.
3. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник / М.В. Бем, І.М. Городиський, Г. Саттон, О.М. Родіоненко. К.: К.І.С., 2015. 220 с.

ПЕРЕЛІК НОРМАТИВНО-ПРАВОВИХ АКТІВ

1. Про доступ до публічної інформації: Закон України від 08.10.2023 р. №2614-IX. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314.