НАЦІОНАЛЬНА АКАДЕМІЯ ПЕДАГОГІЧНИХ НАУК УКРАЇНИ
ДЗВО «УНІВЕРСИТЕТ МЕНЕДЖМЕНТУ ОСВІТИ»
БІЛОЦЕРКІВСЬКИЙ ІНСТИТУТ НЕПЕРЕРВНОЇ ПРОФЕСІЙНОЇ ОСВІТИ

КАФЕДРА ТЕХНОЛОГІЙ НАВЧАННЯ, ОХОРОНИ ПРАЦІ ТА ДИЗАЙНУ

ЕЛЕКТРОННИЙ НАВЧАЛЬНИЙ КУРС

«Безпека в цифровому просторі»

СХВАЛЕНО
на засіданні кафедри технологій навчання, охорони праці та дизайну
протокол № 2 від «06» лютого 2024 р.

Завідувач кафедри _____ Кравченко Г.Ю.

Біла Церква 2024

Затверджено на засіданні кафедри технологій навчання охорони праці та дизайну від 06.02.2024 року № 2

Авторка-розробниця:
Головко Дар'я Юріївна – старша викладачка кафедри технології навчання, охорони праці та дизайну Білоцерківського інституту неперервної професійної освіти ДЗВО «УМО» НАПН України.

Головко Д.Ю. Бепек в цифровому просторі : електронний навчальний курс / Д.Ю. Головко. Біла Церква : БІНПО ДЗВО «УМО» НАПН України, 2024 р. 54 с.

Електронний навчальний курс спрямований на ознайомлення слухачів із сучасними видами кіберзагроз та методами захисту від них, формування навичок безпечного використання цифрових технологій в особистому та професійному житті. В той же час, курс спрямований на розуміння широкого спектру сучасних викликів у сфері цифрової безпеки, а також на формування мінімізації розпізнавання нових потенційних загроз та заходів адаптації до динамічного цифрового середовища.

Метою курсу є надання основних знань та навичок в області кібербезпеки, спрямованих на безпечне та відповідальне використання цифрових технологій в професійній сфері, забезпечуючи їхню готовність ефективно захищати інформаційні ресурси та протидіяти кіберзагрозам у сучасному цифровому середовищі.

Курс розроблено для педагогічних працівників закладів професійної (професійно-технічної) освіти галузі знань 01 «Освіта» на всіх етапах курсів підвищення кваліфікації за різними моделями навчання (очною, заочною, очно-дистанційною, дистанційною).

Курс розраховано на 8 год., із яких 2 год. – лекція, 4 год. – семінарські заняття, 2 год – самостійна робота.

ЗМІСТ

АНОТАЦІЯ

У сучасному цифровому світі все більше уваги приділяється питанням кібербезпеки та захисту персональних даних. Цифровізація суспільства призвела до появи нових загроз, пов'язаних з використанням інформаційних технологій. Тому важливо формувати у громадян необхідні компетентності для безпечної поведінки в цифровому середовищі.

Електронний навчальний курс спрямований на ознайомлення слухачів із сучасними видами кіберзагроз та методами захисту від них, формування навичок безпечного використання цифрових технологій в особистому та професійному житті. В той же час, курс спрямований на розуміння широкого спектру сучасних викликів у сфері цифрової безпеки, а також на формування мінімізації розпізнавання нових потенційних загроз та заходів адаптації до динамічного цифрового середовища.

Програма курсу включає вивчення правил кібергігієни, способів захисту особистих даних, розпізнавання шахрайства в мережі Інтернет, використання засобів захисту пристроїв та програмного забезпечення. Окрема увага приділяється вивченню бнзпечної поведінки в соціальних мережах, використанню сучасних засобів захисту особистих даних в Інтернеті, фішингу та кібершахрайству. Також розглядаються питання захисту пристроїв від шкідливого програмного забезпечення, налаштування безпечних паролів, резервного копіювання даних. В результаті проходження курсу учасники отримають юазові знання та практичні навички з інформаційної безпеки, необхідних для захисту власних інтересів у цифровому просторі.

Теоретичні й практико-зорієнтовані аспекти курсу спрямовано на неперервне підвищення педагогічної майстерності педагогічних працівників. Зокрема, на розвиток *освітологічної, андрагогічної, професійно-педагогічної, інноваційної та інформаційно-цифрової* компетентностей та компетентності з *професійно-особистісного розвитку* педагогічних працівників.

Курс розроблено для педагогічних працівників закладів професійної (професійно-технічної) освіти галузі знань 01 «Освіта» на всіх етапах курсів підвищення кваліфікації за різними моделями навчання (очною, заочною, очно-дистанційною, дистанційною).

Курс розраховано на *8 год.*, із яких 2 год. – лекція, 4 год. – семінарські заняття, 2 год – самостійна робота.

ТИПОВА ОСВІТНЯ ПРОГРАМА ЕЛЕКТРОННОГО КУРСУ

Пояснювальна записка

Актуальність електронного курсу *«Безпека в цифровоу просторі»* визначається стрімким розвитком цифрових технологій у сучасному суспільстві. Зростаюча залежність від інформаційних систем вимагає і навичок безпечного застосування цирових ресурсів, зокрема компетентностей із кібербезпеки. Останні є вкрай важливими для ефективної роботи в вебсередовищі, враховуючи збільшення кількості кіберзагроз та кібератак. Навичик захисту інформації стають пріоритетними для забезпечення стабільності й успішності в сучасній професійній діяльності.

У зв'язку з цим педагоги потребують формування компетентностей щодо безпечної роботи та навчання в цировому середовищі. Вміння ідентифікувати загрози, оцінювати ризики та використовувати ефективні методи захисту даних дозволяють педагогам забезпечити освітній процес та формувати у здобувачів освіти культуру цифрової гігієни і безпеки. Оволодіння сучасними підходами до забезпеченя кібербезпеки сприятиме запобіганню витоку персональних даних здобувачів освіти, пошкодження цілісності інформації та переривання доступу до освітніх ресурсів, що матиме позитивний вплив на якість і безперервність освітнього процесу.

Враховуючи ці аспекти, електронний курс стає важливим інструментом для професійного розвитку педагогів в умовах цифрової трансформації освіти. Він сприятиме формуванню сучасного безпечного освітнього середовища та підготовці до відповідальної поведінки в цифровому просторі.

Метою курсу є надання основних знань та навичок в області кібербезпеки, спрямованих на безпечне та відповідальне використання цифрових технологій в професійній сфері, забезпечуючи їхню готовність ефективно захищати інформаційні ресурси та протидіяти кіберзагрозам у сучасному цифровому середовищі.

Завдання курсу:

- ✓ надати фундаментальні знання у сфері кібербезпеки
- ✓ формувати розуміння техноогій інформаційної безпеки;
- ✓ підвищити рівень цифрової грамотності слухачів;

Навчально-методичне забезпечення курсу представлено науково-методичними матеріалами (лекція, семінарські заняття, завдання для самостійної роботи, тести) і списком рекомендованих джерел до тематики електронного курсу.

ПРОФІЛЬ ТИПОВОЇ ОСВІТНЬОЇ ПРОГРАМИ
ЕЛЕКТРОННОГО НАВЧАЛЬНОГО КУРСУ

Профіль Типової освітньої програми електронного курсу *«Безпека в цифровому просторі»*		
Обсяг курсу		**0,27 ЄКТС кредиту** **На опанування матеріалів електронного курсу передбачено 8 академічних годин**, що відповідає **0,27 ЄКТС кредиту**.
Рівень програми		Безперервний професійний розвиток фахівців шляхом формальної, неформальної та інформальної освіти.
А	**Мета**	
	Надання основних знань та навичок в області кібербезпеки, спрямованих на безпечне та відповідальне використання цифрових технологій в професійній сфері, забезпечуючи їхню готовність ефективно захищати інформаційні ресурси та протидіяти кіберзагрозам у сучасному цифровому середовищіцій у сфері управління безпекою праці на основі ризикорієнтованих підходів.	
В	**Характеристика типової програми**	
1.	Функціональна спрямованість	Неперервне підвищення педагогічної майстерності та розвиток професійних компетенцій слухачів курсів підвищення кваліфікації
2.	Фокус Типової програми	Акцент на розвиток ключових компетентностей фахівців із питань: - поглиблення знань у сфері інформаційної безпеки та кіберзахисту; - практичного застосування основ безпеки в цифровому освітньому середовищі; - опанування практичних навичок використання елементів захисту інформації в освітньому процесі; - розвиток цифрових компетентностей педагогічних працівників; - набуття практичного досвіду щодо застосування заходів для забезпечення захищесності інформаційних систем..
3.	Орієнтація Типової програми	Типова програма електронного курсу орієнтовна на розвиток загальних і фахових компетентностей

		педагогічних працівників ЗП(ПТ)О в умовах формальної, неформальної та інформальної освіти
4.	Особливості типової програми	Типова програма електронного навчального курсу спрямована на розвиток фахової компетентності педагогічних працівників ЗП(ПТ)О, які володіють широким спектром професійних навичок і компетенцій для успішного виконання своїх професійних функцій
5.	Цільова група	Електронний курс розроблено для педагогічних працівників закладів професійної (професійно-технічної) освіти галузі знань 01 «Освіта» на всіх етапах курсів підвищення кваліфікації за різними моделями навчання (очною, заочною, очно-дистанційною, дистанційною).
C	**Професійні вимоги (компетенції) і продовження навчання**	
1.	Професійні вимоги (компетенції)	Визначає посадова інструкція фахівця
2.	Продовження навчання	Типова програма передбачає можливість подальшого розширення та поглиблення знань, умінь, навичок педагогічних працівників ЗП(ПТ)О в системі формальної, неформальної та інформальної освіти.
D	**Стиль і методика навчання**	
1.	Підходи до викладання і навчання	Розвиток загальних і фахових компетентностей педагогічних працівників ЗП(ПТ)О у процесі їх практичного застосування, оновлення і поповнення професійних знань. Навчання проходить за різними моделями (очною, заочною, очно-дистанційною, дистанційною) із використанням компетентнісного, андрагогічного, особистісно-орієнтованого, діяльнісного підходів та інноваційних технологій навчання: інтерактивних, проблемних, кейс-технологій, практичних завдань, тестів тощо.
2.	Система оцінювання	Результати навчання за Типовою програмою оцінюються (зараховано/не зараховано) на основі: підготовки відповідей на проблемно-пошукові питання, виконання завдань самостійної роботи, виконання тестових завдань.
E	**Програмні компетентності**	
1.	Інтегральна компетентність	здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у сфері професійної діяльності або в процесі навчання, що передбачає проведення дослідження, використання теорій і методів менеджменту, педагогіки і психології на практиці
2.	Загальні компетентності *Освітологічна*	здатність інтегрувати знання із сучасної філософії та соціології освіти, освітньої політики й економіки освіти в цілісну стратегію професійної діяльності на засадах

		людиноцентризму, демонструвати відповідні цінності професійної діяльності
3.	Спеціальні (фахові) компетентності	***андрагогічна компетентність*** – уміння визначати освітні потреби і запити, ураховувати особливості мотивації, процесу навчання, визначати результати навчання, спонукати до рефлексії; ***предметно-методична*** – використання у професійній діяльності системи наукових і методичних знань, умінь з основ охорони праці та безпеки життєдіяльності, уміння проводити навчальні заняття ефективно; ***інформаційно-цифрова*** – передбачає впевнене, а водночас критичне застосування інформаційно-комунікаційних технологій для створення, пошуку, обробки, обміну інформацією на роботі, в публічному просторі та приватному спілкуванні; ***професійно-педагогічна*** – здатність планувати, організовувати та контролювати діяльність суб'єктів освітнього процесу закладів професійної освіти та власну професійну діяльність в умовах реформ і соціальних трансформацій; здатність до вибору оптимальних прийомів, методів та форм навчання, застосування інноваційних технологій на основі володіння технологіями створення сприятливих умов для навчального процесу; ***інноваційна*** – система мотивів, знань, умінь, навичок, особистісних якостей педагога, що забезпечує ефективність використання нових педагогічних технологій у роботі зі здобувачами освіти; ***компететність з інформальної освіти та професійно-особистісного розвитку*** – здатність організовувати професійний саморозвиток, самонавчання, самовдосконалення і самореалізацію впродовж життя шляхом формальної, неформальної та інформальної освіти; розвивати (саморозвивати) і вдосконалювати (самовдосконалювати) професійно важливі якості особистості, цінності, що спрямовані на всебічний розвиток особистості всіх суб'єктів освітнього процесу як найвищої цінності суспільства тощо; ***педагогічне партнерство*** – вміння організовувати навчання на засадах дитиноцентризму та індивідуального підходу до кожного здобувача освіти; ***проєктувальна*** – заснована на знаннях, уміннях, особистісному досвіді і ціннісних орієнтаціях педагога, які сприяють ефективній підготовці та впровадженню освітніх проєктів;

		ініціативність і підприємливість – уміння генерувати нові ідеї й ініціативи та втілювати їх у життя з метою підвищення як власного соціального статусу та добробуту, так і розвитку суспільства і держави.
F	**Програмні результати навчання**	
	Знання і розуміння	– розуміння загроз та ризиків, пов'язаних із використанням цифрових технологій у професійнй освіті; – засвоєння базових принципів захисту інформації та даних; – розуміння принципів безпеки в мережах під час взаємодії з іншими користувачами; – розуміння важливості захисту особистих даних та приватності в цифровому середовищі; – розуміння вимог законодавства щодо цифрової безпеки та відповідального використання технологій; – положення про навчання неповнолітніх професіям, пов'язаним із небезпечними, важкими і шкідливими роботами
	Розвинені вміння	- здатність ефективно захищати особисті дані в мережі Інтернет; використовуючи паролі та двоетапну аутентифікацію; - вміння визначати потенційні загрози в мережі Інтернет, такі як фішингові атаки, віруси та інші види кіберзлочинності; - здатність розпізнавати та запобігати онлайн-залякуванню; - вміння розробляти та впроваджувати плани дій у випадку кібератак;
	Диспозиції (цінності, ставлення)	- морально-етичні; - соціально-політичні; - людиноцентризм; - готовність до змін, гнучкість, постійний професійний розвиток; - необхідність володіння нормативно-правовою базою з цифрової безпеки; - пріоритет життя і здоров'я працівників та здобувачів освіти закладів професійної освіти - рефлексія власної професійної діяльності
Ключові слова Кібербезпека, кібератака, кіберзагроза, кіберзлочин, кіберзахист, цифрові технології, захист персональних даних, антивірусний захист, шифрування, соціальна інженерія, кібергігієна, аутентифікація, фішинг.		

ТЕМАТИЧНИЙ ПЛАН ВИКЛАДУ І ЗАСВОЄННЯ МАТЕРІАЛІВ ЕЛЕКТРОННОГО НАВЧАЛЬНОГО КУРСУ

Тематичний план	**Форми роботи, кількість годин**					
	Усього годин	Лекції	Семінарське заняття	Самостійна робота	К-сть годин контролю	Вид контролю
Тема 1 «Кіберебезпека в цифровому просторі»	4	2	2			
Тема 2 «Нормативно-правові засади забезпечення безпеки цифрового простору»	2		2			
Тема 3 «Розвиток культури кібербезпеки у цифровому просторі»	2			2		
Разом	**8**	**2**	**4**	**2**		

ЗМІСТ ЕЛЕКТРОННОГО НАВЧАЛЬНОГО КУРСУ ЗА ТЕМАМИ

Тема 1. Кібербезпека в цифровому просторі

Поняття кіберпростору, кібербезпеки та кіберзагрози в цифровому середовищі. Напрями кібербезпеки. Принципи конфіденційності, цілісності та доступності даних.

Види кібератак та кіберінцидентів. Наслідки порушення безпеки в інформаційному просторі. Способи ідентифікація особи. Персональні дані та місця їх зберігання. Причини крадіжки даних. Збереження та захист персональних даних.

Соціальна інженерія та кібербезпека. Навчання та безпечний Інтернет. Забезпечення безпеки мережевих інфраструктур навчальних закладів.

Хакерські атаки. Інтернет-браузер, месенджери, оціальні мережі та кібербезпека.

Тема 2. Нормативно-правові засади забезпечення безпеки цифрового простору в ЗП(ПТ)О

Українське законодавство у сфері кібербезпеки та захисту інформації. Правове регулювання використання інформаційно-комунікаційних технологій в освітньому процесі.

Юридична відповідальність за правопорушення у сфері кібербезпеки. Правовий аспект протидії кібербулінгу та іншим інтернет-ризикам. Порядок реагування ЗП(ПТ)О на кіберінциденти.

Авторське право та ліцензування програмного забезпечення. Правові наслідки плагіату та піратству в цифровому просторі. Міжнародне зконодавство у фері забезпечення кібербезпеки освіти.

Тема 3. Формування культури кібербезпеки в освітньому середовищі

Поняття культури кібербезпеки. Правила цифрової гігієни та етики.

Критичне мислення та медіаграмотність для оцінки кіберризиків. Методи розпізнавання фейків. Аналіз поштового повідомлення.

.

ТЕОРЕТИЧНИЙ НАВЧАЛЬНИЙ МАТЕРІАЛ

ІНТЕРНЕТ-ЛЕКЦІЯ

Тема: «Кібербезпека в цифровому просторі»

Мета: формувати чітке розуміння кіберпростору, розкрити основні аспекти кібербезпеки та її загроз, розвинути відповідальне ставлення до цифрової безпеки.

Основні поняття: кіберпростір, кеіберзагроза, кіберзахист, конфіденційність цілісність, доступність, фішинг, вішиг, дорожнє яблуко, троянський кінь, соціальна інженерія.

Уміння, які мають бути вироблені, та навички, які мають бути напрацьовані під час заняття: аналізувати та ідентифікувати кіберзагрози в освітньому середовищі, оцінювати ризики порушення кібербезпеки, застосовувати оптимальні методи та засоби захисту забезпечення кіберзахисту, розробляти рекомендації щодо підвищння рівня кібербезпеки,

План

1. Поняття кіберпростору, кібербезпеки та кіберзагрози.
2. Основні аспекти кібербезпеки.
3. Загрози учасникам освітнього процесу у кіберпросторі.
4. Забезпечення кібербезпеки навчального процесу.

Питання для самоконтролю

1. Що таке «кіберпростір» та «кібербезпека»?
2. Які загрози існують для учасників освітнього процесу в кіберпросторі?
3. Як можна забезпечити кібербезпеку навчального процесу?
4. Які методи кіберзахисту є найбільш ефективними?
5. Які рекомендації можна надати для підвищення рівня кібербезпеки в освітньому закладі?

Матеріали лекції

---

1. Поняття кіберпростору, кібербезпеки та кіберзагрози

Кіберпростір – середовище (віртуальний простір), яке надає можливості (послуговує) здійсненню комунікацій та/або реалізації суспільних відносин, утворене внаслідок функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням Інтернет та/або інших глобальних мереж передачі даних.

Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, за якого забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Проєкт ЗУ від 14.04.2016 № 2126а «Про основні засади забезпечення кібербезпеки України»

Кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, мають негативний та/або послаблюючий вплив на стан кібербезпеки України, кібербезпеку та кіберзахист її об'єктів;

Важливість кіберпростору для життя сучасного суспільства є очевидною, зважаючи не лише на такі показники, як кількість користувачів мережі Інтернет та динаміка їх збільшення, але й поступове проникнення його у решту сфер людського життя.

Кіберпростір – інтерактивне інформаційне середовище, яке функціонує за допомогою комп'ютерних систем. Іншими словами – це просто віртуальний простір, який дозволяє людям взаємодіяти між собою та реалізовувати суспільні відносини: спілкування, навчання, купівлі будь-яких товарів, ведення бізнесу, розваги, державні комунікації, зв'язок.

Кіберпростір можна розглядати як тріаду, до якої входять:

1) інформація у своєму цифровому представленні: статична (файли, записані на носії інформації) тадинамічна (пакети, потоки, команди, запити тощо);

2) технічна інфраструктура: ІКТ, програмне забезпечення, бази даних та бази знань;

3) інформаційна взаємодія суб'єктів з використанням отриманої (переданої) інформації та обробки через технічну інфраструктуру.

Можливості людей в кіберпросторі неймовірні. Проте варто знати, що на всіх в кіберпросторі чатує безліч небезпек. Всі ризики, які ви можете уявити в реальному житті, є в кіберпросторі. Ризики у віртуальному просторі не менші, ніж у реальному світі, включно навіть з тими, що загрожують життю і здоров'ю людини. Ці ризики дуже швидко переростають у загрози через специфіку самого кіберпростору, тому що їх можна доставити та реалізувати набагато швидше, не маючи фізичного контакту:

- шахрайство;
- булінг;
- психологічний вплив;
- фінансові ризики;
- ризики, пов'язані з майном;
- ризики, пов'язані з життям тощо.

Розвиток технологій весь час підвищує рівень небезпеки у кіберпросторі. Кіберзагрози у сучасному суспільстві набирають значного масштабу. Відтепер успішна атака хакерів може знеструмити цілу область або країну, призвести до пограбування банку чи знищити успішну організацію. Нехтування питаннями кіберзахищеності на тлі зростаючих кіберзагроз є вкрай небезпечним, а ціна такого ігнорування є надто високою. Так, 2021 року середня глобальна вартість злому даних склала 4,24 млн доларів США, що перевищило середні витрати на злом даних у $3,86 млн у попередньому році.

Кібератаки спрямовані на пошкодження важливих документів і систем у корпоративній або персональній комп'ютерній мережі, а також отримання доступу до них. Кібератаки здійснюють як окремі особи, так і цілі організації в політичних, кримінальних або особистих цілях для знищення засекреченої інформації чи отримання доступу до неї.

Кібератаки на комп'ютерні мережі та системи відбуваються по-різному. Шкідливе програмне забезпечення та фішинг – це два приклади кібератак, які використовуються для отримання контролю над делікатними даними з корпоративних і персональних електронних пристроїв.

Шкідливе програмне забезпечення, або програми, створені зловмисниками, – це замасковані під надійне джерело вкладення електронної пошти або програми (наприклад, зашифрований документ або папка з файлами), які використовуються для поширення вірусів і дають кіберзлочинцям змогу проникнути в комп'ютерну мережу. Цей тип кібератаки часто вражає всю IT-мережу. Приклади шкідливого програмного забезпечення: троянські програми, шпигунське програмне забезпечення, хробаки, віруси та рекламне ПЗ.

DDoS-атаки – це тип атак, під час яких кілька хакерських комп'ютерних систем уражають сайти або мережі так, що вони стають недоступними для користувачів. Наприклад, сотні спливаючих рекламних оголошень і навіть збої в роботі сайту можуть сприяти поширенню DDoS-атак на враженому сервері.

Фішинг – це надсилання шахрайських електронних листів від імені авторитетних компаній або інших надійних джерел. Зловмисники використовують фішинг, щоб отримувати доступ до даних у персональній або корпоративній мережі.

SQL-ін'єкції – це спосіб поширення шкідливого ПЗ через програми, як-от LinkedIn і Target, який дає змогу кіберзлочинцям викрадати або видаляти дані, а також керувати ними.

Міжсайтові сценарії полягають у тому, що кіберзлочинець надсилає заспамлені або вражені сценаріями посилання на вашу електронну пошту. Щойно ви їх відкриваєте, зловмисник отримує ваші персональні дані.

Бот-мережі. Принцип дії бот-мереж: зловмисники вражають кілька комп'ютерів, підключених до приватної мережі, вірусами або іншими формами шкідливого програмного забезпечення, як-от спливаючими повідомленнями чи спамом.

Зловмисні програми з вимогою викупу – це програми, створені зловмисниками, які порушують або блокують доступ жертви до важливих даних і систем, доки вона не спла

Використання надійного програмного забезпечення й ефективна кіберстратегія можуть знизити ймовірність кібератаки на корпоративну або особисту базу даних.

Завдяки стрімкому розвитку цифрових пристроїв та «розумних» ґаджетів, а також збільшенню обсягів інтернет-трафіку та потоків даних, люди почали переносити дедалі більше персональної інформації у віртуальний простір – зокрема, у соціальні мережі та хмарні сховища на кшталт Google Drive чи iCloud. Це можуть бути особисті дані, фото- та відеоматеріали, дані банківських карт чи документів. У зв'язку з цим зросла потреба у захисті даних в інтернеті, а питання кібербезпеки набули ще більшої актуальності.

Кібербезпека – це застосування технологій, процесів та засобів для захисту систем, мереж, програм, пристроїв та даних від кібератак.

Кібербезпека включає в себе:

- ✓ захист інформації від вірусів, хакерських атак, підробки даних, які можуть призвести до їхнього видалення/викрадення, використання інформації проти людини, що може вплинути на її життя в цілому;
- ✓ захист систем, процесів та людей.

Системи: засоби комп'ютерної безпеки, які необхідні для захисту від кібератак. Захищати слід комп'ютери, розумні пристрої, маршрутизатори, мережі та хмари через брандмауери нового покоління, фільтрацію DNS, захист від шкідливих програм, антивірусне програмне забезпечення.

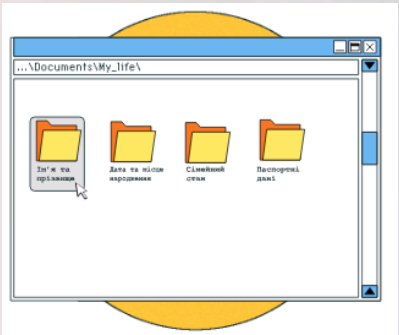
Процеси: правила та норми для виявлення атак і загроз, способів реагування на них та захисту систем, а також відновлення після успішних атак.

Люди: користувачі повинні розуміти та дотримуватися основних принципів безпеки даних, таких як вибір надійних паролів, обережність щодо вкладень в електронній пошті, резервне копіювання даних тощо.

Кібербезпека покликана захистити дані (зокрема, персональні дані) на етапі їхнього обміну та збереження під час користування будь-яким пристроєм.

Персональними даними (*англ. personal data*) називають будь-яку інформацію, що дозволяє ідентифікувати користувача в реальному житті:

- ім'я та прізвище;
- дату та місце народження;
- сімейний стан;
- паспортні дані;
- дані про професію тощо.



Водночас паролі та облікові записи самі по собі не відносяться до персональних даних, оскільки не містять конкретної інформації про людину.

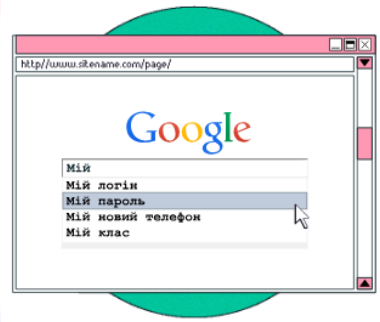
Використовуючи Інтернет для спілкування, планування зустрічей чи подорожей, отримання новин тощо, ми ділимося даними, що детальніше описують нас як особистість. Все це формує нашу цифрову ідентичність.

Цифрова ідентичність (або ідентичність онлайн) – це сукупність інформації, дані, які унікально описують особу та яку можна отримати в результаті онлайн-діяльності.

До такої інформації належать:

- імена користувачів;
- паролі;
- операції пошуку в Інтернеті;
- дата народження;
- історія покупок тощо.

Цифрова ідентичність є віртуальним відображенням реальної соціальної ідентичності людини, або іншими словами – ідентифікацією в Інтернеті.



Пошук Google Google зберігає історію пошукових запитів користувачів. Ці дані часто використовуються власниками сайтів та рекламодавцями для відстеження людей в мережі, аби надавати їм персоналізовану інформацію та рекламу.

У реальному житті людина контролює свої персональні дані: вона розкриває їх лише тим, кому бажає, та лише у випадку необхідності. Інша сторона може перевірити достовірність цих даних. Проте в Інтернеті з'являється третя сторона – ті, хто збирає, зберігає та передає дані. Тим самим користувач втрачає контроль над власною інформацією.

Навіть невеликі дії в мережі та поза нею формують «цифровий слід», який позбавляє анонімності та конфіденційності. Створення облікових записів, паролів, перегляд сторінок – все це зберігається та утворює цифровий слід користувача.

Спілкуючись у соціальних мережах, ми часто відчуваємо довіру до співрозмовника. Іноді ділимося з ним особистою чи навіть інтимною інформацією у приватних повідомленнях, оскільки не хочемо оприлюднювати її. Натискаючи «відправити», здається, що це безпечно – адже завжди можна видалити повідомлення чи файл. Деякі месенджери навіть дозволяють видалити інформацію з переписки обох учасників. Проте чи насправді це гарантує конфіденційність?

На жаль, все, що потрапило в мережу, там назавжди залишається. З видаленого повідомлення можуть зробити скріншот, а фото зберегти. Навіть якщо ви цілком довіряєте людині, котрій надсилаєте приватну інформацію, пам'ятайте – цифровий слід залишиться назавжди.

2. *Основні аспекти кібербезпеки*

Але якщо така інформація вже оприлюднена, її треба захистити.

1. Використовуйте безпечне з'єднання

- Якщо планується використовувати особисті дані в Інтернеті, потрібно переконатися, що з'єднання захищене. Краще користуватися домашньою мережею або мобільним зв'язком.
- Уникайте відкритих Wi-Fi мереж без пароля. Відвідуйте сайти, адреса яких починається з https://. Літера «s» означає, що з'єднання безпечне. Дані, які передаються таким захищеним каналом (фото, відео, повідомлення), шифруються. Навіть якщо їх перехоплять, без ключа дешифрувати майже неможливо.

2. Подбайте про безпеку своїх пристроїв

- Встановіть надійний антивірус для захисту від шкідливих програм та регулярно проводьте повне сканування комп'ютера.
- Постійно оновлюйте інтернет-браузер, програми та додатки на гаджетах – це дозволить виправити уразливості та помилки в програмному забезпеченні.
- Завантажуйте програми лише з офіційних джерел.
- Проаналізуйте вже встановлені додатки, видаліть непотрібні та надалі контролюйте процес установлення.
- Звертайте увагу на дозволи, які запитують додатки. Часто шкідливі програми вимагають зайвих дозволів для збору інформації про користувача. Виходьте зі своїх профілів, особливо при використанні чужих пристроїв.

3. Перевірте безпеку вже наявних облікових записів електронної пошти та соціальних мереж

Спеціальні сайти, наприклад haveibeenpwned.com та breachalarm.com, допоможуть повністю з'ясувати, чи були скомпрометовані паролі до електронної пошти та інших акаунтів.

4. Не відкривайте та не завантажуйте підозрілі повідомлення та посилання

Перш ніж перейти за посиланням, зверніть увагу на адресу сайту, а не лише на зовнішній вигляд. Часто зловмисники створюють точну копію відомого ресурсу для збору персональних даних користувачів. Про такі шахрайські сайти-двійники попереджають офіційні сторінки та акаунти брендів.

5. Використовуйте надійні паролі

Важливо створити складну комбінацію не менше ніж з 12 символів, що містить великі й малі літери, цифри та спецсимволи. Деякі системи вимагають мінімум 6 символів, але чим довший пароль, тим він безпечніший. Уникайте очевидних даних, таких як номер телефону, дата народження, адреса, імена домашніх улюбленців тощо. Використовуйте різні паролі для різних акаунтів та не зберігайте їх у браузері. Повторне використання паролів полегшує злам. Для зручності можна використовувати мнемонічні фрази чи менеджери паролів. Вони генерують складні паролі та безпечно зберігають їх.

Ось кілька способів створити й запам'ятати надійний пароль:

- ✓ *Використати дитяче слово.* Пригадайте якесь слово, яке ви вигадали і якого немає в словнику. Наприклад «бумблік». Ви можете використати його як основу для пароля, додавши цифри та символи: bumbL1k#
- ✓ *Зробити акронім з фрази.* Візьміть фразу із вірша, пісні чи цитати. Наприклад: «Сонце сходить і заходить». Зробіть з неї акронім, тобто візьміть по першій ліері кожного слова. Потім запишіть латиницею і додайте симфоли та цифри: SsIz#21
- ✓ *Ввести випадкові символи.* Ніби помилково змініть розкладку клавіатури і надрукуйте кілька випадкових символів. Потім додайте літери, цифри для підсилення. Наприклад: No9Jpe781
- ✓ *Намалювати візуальний ключ на клавіатурі.* Уявіть, що ви малюєте пароль пальце на сенсорній клавіатурі смартфона. Наприклад, проведіть пальцем по літерах Q, W, E, R, T,Y. Додайте цифри і символи для посилення: QwertY@09

За даними досліджень, найлегше зламуються такі поширені паролі:

- 123456,
- password,
- 123456789,
- 12345678,
- 12345,
- 111111,
- 1234567,
- sunshine,
- qwerty,
- iloveyou.

6. Встановіть додатковий рівень захисту (двофакторну аутентифікацію)

Для посилення безпеки акаунтів використовуйте двофакторну аутентифікацію. Вона передбачає підтвердження особи через SMS або спеціальний додаток під час входу. Так зловмисники не зможуть отримати доступ до даних навіть за наявності пароля.

7. Слідкуйте за роботою камери і мікрофона

Надавайте доступ до них лише перевіреним додаткам. Регулярно переглядайте дозволи в налаштуваннях браузера.

8. Контролюйте активність банківських і кредитних карт

Регулярно перевіряйте рахунки на наявність підозрілих операцій. Встановлюйте ліміти на різні транзакції. Не повідомляйте дані карток стороннім особам, навіть від імені банку.

9. Захистіть свої конфіденційні дані

Перед тим як викинути чи продати пристрої, впевніться, що там не залишилося особистої інформації – зробіть її нерозбірливою або видаліть.

10. Заведіть декілька електронних скриньок

Використовуйте одну лише для особистого листування, а іншу – для публічного доступу. Не відповідай на спам.

11. Регулярно робіть резервне копіювання

Щоб уникнути втрати важливих даних, систематично зберігайте інформацію на зовнішньому жорсткому диску чи в хмарі. Це допоможе відновити файли після атак шкідливих програм.

12. Контролюйте інформацію, яку публікуєте в соцмережах

Повідомлення, фото чи відео з конфіденційними даними можуть бути використані проти Вас . Мінімізуйте особисту інформацію про себе та близьких, не повідомляй її на запити від імені банків тощо.

13. Робіть покупки в Інтернеті безпечно

Не повідомляйте тризначний код карти, паролі від банкінгу. Використовуйте віртуальні картки та перераховуйте на них лише потрібну суму. Перевіряй продавців/покупців у сервісі Кіберполіції «STOP FRAUD» та наявність сайту в Black List ЄМА (*www.ema.com.ua/blacklist/*). Будьте уважними під час оплати.

Ось альтернативний варіант тексту:

Якщо виникла підозра про викрадення даних або була спроба зламу:

1. Скиньте або вимкніть одночасні сесії, якщо вони були увімкнені.
2. Негайно змініть усі можливі паролі на всіх акаунтах.
3. Перевірте акаунти антивірусною програмою.
4. Якщо була спроба викрасти банківські дані, негайно повідомте банк і заблокуйте рахунки/картки.
5. У разі шахрайства телефонуйте на гарячу лінію Кіберполіції за номером 0 800 505 170.

3. Загрози учасникам освітнього процесу у кіберпросторі

Спектр загроз кіберпростору постійно розширюється. Якщо 10 років тому небезпеки для учнів обмежувалися вірусними атаками, кіберзлочинністю та ризиками інтернет-серфінгу, то зараз їх різноманіття зростає, охоплюючи всі сфери діяльності людини в мережі. Найбільшу загрозу для школярів становлять приховані активні небезпеки.

Активне використання мереж, особливо дітьми та молоддю, призводить до збільшення різних видів загроз з мережі. Ця проблема особливо гостро постає при створенні та використанні соціальних мереж. Найбільш активні приховані загрози для дітей в комп’ютерній мережі можна класифікувати так:

– вірусні атаки;

– кіберзлочинність (спам, кардинг, фішинг тощо);
– загрози від мережевого серфінгу (кібербулінг, небезпечний контент, порушення приватності тощо).

Взаємодію школярів з мережею можна розглядати як систему «Людина-техніка-середовище». Тут мережа – це машина, що впливає на людину як загроза. Відповідно, «мережевий ефект» проявляється через помилки користувача, вплив ігор, інтернет-залежність.

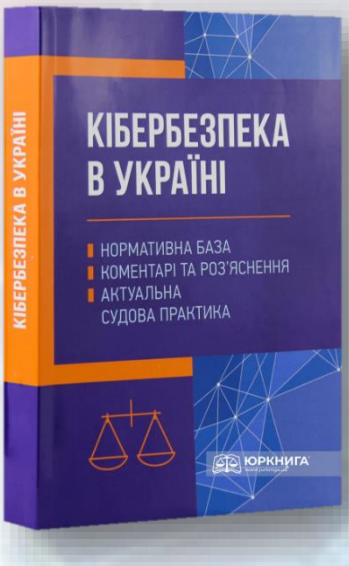
Загрози з мереж можна поділити на: активні/пасивні, відкриті/приховані, поточні/відкладені. За допомогою ергономічного підходу активні небезпеки можна оцінити як ієрархію показників.

Згідно із Законом України «Про основні засади забезпечення кібербезпеки України», сфера освіти не належить до критичних галузей захисту. Проте сучасні учні та студенти в майбутньому можуть працювати в таких галузях. Тому вони потребують захисту, відповідної підготовки та розуміння можливих цільових груп кібербезпеки, наприклад:

– учні/студенти;
– викладачі;
– діти/молодь;
– населення загалом.

За засобами дії проблеми кібербезпеки можна класифікувати так:

– правові;
– технічні;
– інформаційні;
– організаційні;
– психологічні.



Інформаційні засоби класифікуються за завданнями користувачів:

– захист
– інформування;
– зміст;
– навчання;
– безпека;
– життєстійкість;
– уникнення загроз.

Можливі *цілі впливу* кібербезпеки:

– бази даних;
– персональні дані;
– ЗМІ;
– соціальні мережі;
– освіта;
– підручники.

Організаційні засоби:

– інформування;
– навчання;
– створення та поширення засобів;

– контроль.

Психологічні засоби класифікуються за рівнями: національним, суспільним, груповим, індивідуальним тощо.

Людський фактор є ключовим для ефективності кібербезпеки. Найбільш невідкладні потреби - це психосоціальні, культурні, концептуальні та організаційні аспекти.

4. Забезпечення кібербезпеки навчального процесу

Згідно з останніми дослідженнями кібербезпеки, інформаційно-технічні засоби в цій сфері постійно вдосконалюються, а хакерські атаки переорієнтовуються більше на людину, ніж на техніку. Це особливо важливо враховувати через гостроту питання особистої безпеки людини та результатів її діяльності.

Під час роботи в інформаційному середовищі людина стає не лише суб'єктом, а й об'єктом діяльності інших учасників інформаційного простору. Людська відкритість є результатом цілей діяльності: використовуючи інформацію як інструмент, людина має «торкнутися» до неї, зв'язатися з нею. У цей момент людина стає відкритою для інформації та вразливою від неї.

Зміщення цілей кіберзлочинності з технічних об'єктів на людську ланку призвело до появи соціальної інженерії – методів отримання доступу до інформації, заснованих на маніпуляції людською психологією. Основними типами соціальної інженерії є:

Претекстинг – дії за заздалегідь підготовленим сценарієм для отримання потрібної інформації або примушення жертви до певних дій. Спочатку збираються дані про людину, а потім використовуються для входження в довіру.

Фішинг – інтернет-шахрайство для здобуття конфіденційних даних користувача. Найпоширеніше – підроблений лист від імені офіційної установи з формою для введення особистої інформації або посиланням на шахрайський сайт. Такі методи маніпулювання людською довірою та інтересами використовують для незаконного доступу до конфіденційних даних.

Троянський кінь – це хитромудра техніка, яка використовує цікавість, страх чи інші емоції користувачів. Зловмисник надсилає листа жертві електронною поштою із вкладеним «оновленням» антивірусу, ключем до грошового виграшу чи компроматом на співробітника. Насправді, у вкладенні прихована шкідлива програма, яка після запуску на комп'ютері жертви, дозволить зловмиснику збирати чи змінювати інформацію.

Техніка Qui pro quo (послуга за послугу) передбачає звернення зловмисника до користувача електронною поштою чи по робочому телефону. Зловмисник може представитися технічною підтримкою й повідомити про проблеми на робочому місці, що потребують усунення. Під час «вирішення» проблеми, зловмисник підштовхує жертву до дій, які дозволять йому виконати певні команди чи встановити необхідне програмне забезпечення на комп'ютері жертви.

Дорожнє яблуко – це метод, який використовує фізичні носії (CD, флешки), щоб заманити користувача, подібно до троянського коня. Зловмисник підкидає такий носій у загальнодоступних місцях. Щоб викликати інтерес, на носії може бути логотип відомої компанії.

Метод *байтинг* схожий на попередній, а також на фішинг і троянського коня. Відмінність полягає в тому, що байтер може запропонувати користувачеві реальну безкоштовну послугу (музику, фільми тощо) в обмін на конфіденційну інформацію.

При *зворотній соціальній інженерії* зловмисник створює ситуацію, в якій жертва сама звертається до нього по «допомогу». Наприклад, він може викликати тимчасові неполадки в пристрої жертви, а потім проінформувати про службу підтримки. Користувач тоді телефонує чи пише зловмиснику, і під час «усунення» проблеми той отримує потрібні дані.

При *дружніх листах* надсилають електронні листи про отримання спадщини, призів, бонусів чи переказу грошей.

Вішинг – голосова версія фішингу, пов'язана з телефонним шахрайством. Мета – отримати банківські реквізити, конфіденційну інформацію або змусити переказати гроші на рахунок зловмисника.

При методі «*Контакти*» відбувається масова розсилка спаму від імені знайомих користувачів. Іншими словами, заволодівши чиїмось обліковим записом в соціальній мережі чи електронній пошті, кіберзлочинці можуть намагатися надсилати від цього імені шкідливі посилання. Ця психологічна тактика базується на схильності людей довіряти своїм знайомим і відкривати посилання, отримані від них, не замислюючись.

В останні роки методи соціальної інженерії набули широкого застосування для впливу на осіб, що приймають рішення в сферах політики та бізнесу. Розробляються і вдосконалюються рекомендації, методики та засоби протидії соціальній інженерії. Проте практично відсутній розгляд дії та протидії цим методам стосовно освітньої галузі, незважаючи на те, що діти й підлітки дедалі частіше стають об'єктами кібератак через Інтернет. Засоби протидії, розроблені для дорослих, можуть бути поширені і на здобувачів освіти, але з урахуванням їх вікових та діяльнісних особливостей.

Основним способом захисту від методів соціальної інженерії є навчання учасників освітнього процесу. Вони всі (здобувачі освіти, педагоги, організатори навчання) мають бути попереджені про небезпеку розголошення особистої та конфіденційної інформації, а також про шляхи запобігання витоку даних. Крім того, кожен, залежно від своєї ролі в освітньому процесі, повинен мати інструкції щодо того, як і на які теми можна спілкуватися зі сторонніми особами з приводу персональних даних, яку інформацію можна надавати службі техпідтримки, які відомості учасник навчання може повідомляти стороннім та працівникам ЗМІ. Окрім цього, можна виділити дев'ять типових правил протидії соціальній інженерії.

1. *Облікові дані, видані користувачеві, є власністю навчального закладу*. Всім співробітникам у день прийому на роботу має бути роз'яснено, що надані їм логіни і паролі не можна використовувати в інших цілях (на сайтах, для особистої пошти тощо), передавати третім особам чи іншим працівникам без прав доступу. Наприклад, йдучи у відпустку, співробітник не може передати свої дані колезі, щоб той виконав певну роботу чи подивився дані. Персональні дані з результатів тестувань та психологічних і медичних обстежень можуть бути використані зловмисниками, тому потребують обережного поводження.
2. *Потрібно проводити вступні та регулярні тренінги для співробітників і здобувачів освіти*, спрямовані на підвищення знань з інформаційної безпеки. Такі інструктажі дозволять учасникам освітнього процесу мати актуальні дані про існуючі методи соціальної інженерії та не забувати основні правила кібербезпеки.
3. *Обов'язково мають бути регламенти та інструкції з безпеки*, доступні користувачам. У них повинні описуватися дії у різних ситуаціях. Наприклад,

можна прописати алгоритм дій та куди звертатися, якщо стороння особа намагається дізнатися конфіденційну інформацію чи отримати доступ.

4. *На комп'ютерах має бути актуальне антивірусне забезпечення та брандмауер*.
5. *У корпоративній мережі освітніх закладів треба використовувати системи виявлення й запобігання кібератакам*, а також запобігання витоку конфіденційної інформації. Це знизить ризик фішинг-атак.
6. *Права користувачів у системі мають бути максимально обмежені*. Наприклад, можна заборонити доступ до певних сайтів чи використання знімних носіїв поза межами навчального закладу.
7. *Варто бути пильним щодо джерела, яке запитує конфіденційні дані*. Навряд чи представники Міністерства освіти будуть телефонувати до навчального закладу за інформацією про конкретного здобувача освіти чи педагога. Якщо просять ввести особисті дані – краще самостійно зайти на сайт компанії, скажімо банку, чи зателефонувати на офіційний номер установи для уточнення.
8. *Ніколи не варто відкривати вкладення чи переходити за посиланням без вивчення деталей*. Часто в адресах містяться помилки, а посилання виглядають неправдоподібно.
9. Треба *критично ставитися до отриманих повідомлень*: наскільки ймовірно, що принц з Африки чи американський мільярдер можуть заповісти вам спадщину?

Рекомендується попереджати про такі небезпеки інших членів родин, особливо літніх людей, які не мають досвіду користування електронними засобами та обізнаності з питань соціальної інженерії.

Останнім часом в Україні впроваджуються спеціальні навчальні програми та курси для здобувачів освіти та педагогів з безпечного Інтернету. Наприклад, популярний сайт «Онляндія: безпечна веб-країна» та програма Microsoft "Онляндія – безпека в Інтернеті". Проте нові кіберзагрози вимагають нових підходів до захисту користувачів, зокрема учасників освітнього процесу.

Посилання на сайт див. тут

ВІДСКАНУЙТЕ

Для викладачів важливе значення має не лише знання критеріїв надійності джерел та даних, а й використання ефективних педагогічних технологій для формування відповідних умінь учнів і студентів, а також засоби оцінювання рівня розвитку таких умінь.

20 грудня 2002 року Генеральна Асамблея ООН ухвалила резолюцію 57/239 «Принципи створення глобальної культури кібербезпеки». У цьому документі визначено

дев’ять основоположних елементів, які взаємодоповнюють один одного і формують глобальну культуру кібербезпеки:

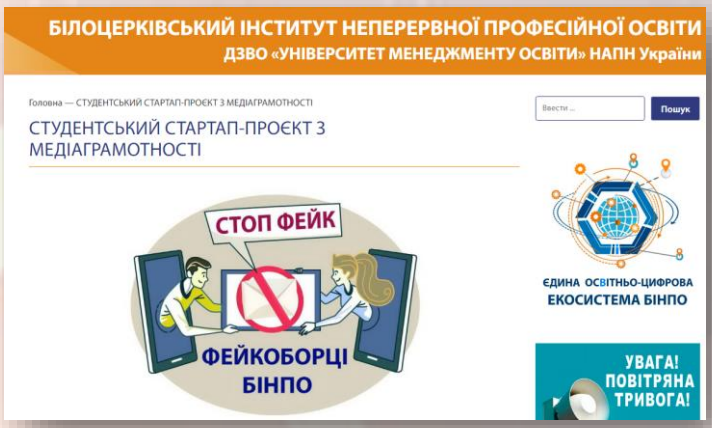
- ✓ освіченість;
- ✓ свідома відповідальність;
- ✓ ефективна реакція;
- ✓ професійна етика;
- ✓ демократичні цінності;
- ✓ оцінка ризиків;
- ✓ розробка та впровадження засобів безпеки;
- ✓ менеджмент безпеки;
- ✓ постійна переоцінка.

Аналіз освітніх програм навчальних закладів країни виявив, що формування критичного мислення здобувачів освіти є ключовим аспектом при вивченні методики викладання навчальних предметів у зв’язку із застосуванням Інтернету. У той самий час, розв’язання проблем безпеки учнів в Інтернеті в розвинених країнах світу, де Інтернет широко використовується в навчальній і науковій діяльності, відзначається комплексним підходом. Проблема безпеки тісно пов’язана з формуванням відповідальності здобувачів освіти за їхні дії чи бездіяльність в мережі для уникнення та/або зменшення ризиків.

Наприклад, у США, Німеччині, Канаді, Фінляндії та інших країнах учні разом з батьками і представниками школи укладають спеціальні угоди щодо безпечного та відповідального використання Інтернету. Ці угоди чітко визначають обов’язки щодо безпечного та відповідального використання соціальних мереж всіма учасниками освітнього процесу.

Найефективніший спосіб протидії проблемам кіберзагроз – розуміти їх сутність і змінювати поведінку. Правила безпеки прості та відомі, і їх слід активно впроваджувати. Варто уважно вивчати власні дії та дії інших учасників освітнього процесу. Розуміти, які небезпечні дії вони здійснюють, наприклад, чи безпечно клікати по посиланнях, покладаючись лише на антивірусний захист? В кіберзагрозливому світі важливе місце повинно займати тренування всіх учасників мережевої діяльності стосовно можливого впливу кіберпростору.

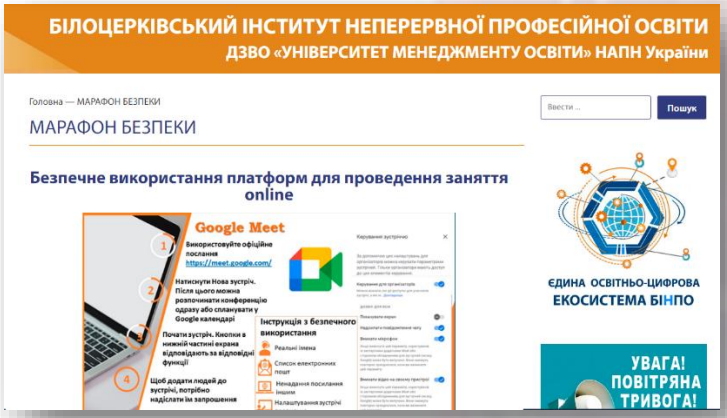
Ефективним інструментом для формування безпечної та відповідальної поведінки педагогів і здолбувачів освіти при використанні Інтернет-ресурсів є проведення спеціальних тренінгів з критичного оцінювання надійності джерел і достовірності даних, що публікуються в мережі. Інструменти і методичні рекомендації для формування таких навичок розміщені на веб-ресурсі «Фейкоборці» (https://binpo.com.ua/).



Посилання на ресурс див. тут

ВІДСКАНУЙТЕ

Сприятливим методом боротьби з кіберзагрозами є використання комп'ютерного моделювання у відносно замкнених системах, таких як корпоративні та навчальні. Навчання «кібер-виживанню» стає важливим елементом відповіді на загрози, що полягає в розпізнаванні та раціональній компенсації можливих небезпек у мережі. Тренування стійкості користувачів відіграє ключову роль у протидії кіберзагрозам, зокрема формування усвідомленого чуттєвого досвіду взаємодії з кіберзагрозами та ефективної реакції на них. Прикладом такого корпоративного навчання є «Марафон Безпеки» (https://binpo.com.ua/)



Посилання на ресурс див. тут

ВІДСКАНУЙТЕ

Важливо зауважити, що досягнення ефективності в розв'язанні завдань забезпечення кібербезпеки можливе лише при систематичному використанні різноманітних засобів на всіх рівнях структури, враховуючи значущість кожного з них для конкретної цільової аудиторії та/або області застосування відповідної системи, орієнтованої на потреби людини.

ПРАКТИЧНІ/СЕМІНАРСЬКІ ЗАНЯТТЯ

СЕМІНАРСЬКЕ ЗАНЯТТЯ 1

Тема: «Кібербезпека у цифровому просторі»

Мета: розвиток самостійного орієнтування в насиченому інформаційному просторі; розпізнавння маніпуляцій та неправдивих даних, що поширюються через інтернет, соціальні медіа, месенджери; навчитися захищати власні персональні дані й протидіяти інформаційним загрозам; долучитися до інформаційної оборони України

Основні поняття: кібергігієна, хакерська атака, веб-браузер, протокол, cookies, месенджер

Уміння, які мають бути вироблені, та навички, які мають бути напрацьовані під час заняття: здійснювати заходи забезпечення інформаційної безпеки, кібербезпеки та захисту персональних даних; використовувати безпечні, сучасні інформаційні та комунікаційні технології; впроваджувати механізми захисту в інформаційному просторі та кіберпросторі; дотримуватися основних принципів інформаційної гігієни для запобігання негативним інформаційно-психологічним впливам.

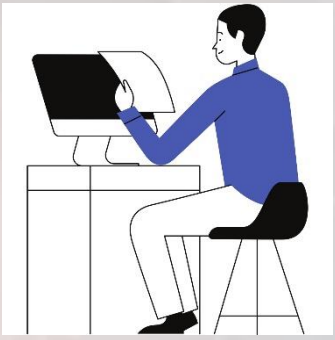
План

1. Поняття кібергігієни.
2. Хакерські атаки.
3. Безпечний веб-браузер.
4. Безпека меседжерів.
5. Безпека соціальних мереж.

Питання для обговорення

1. Поняття кібергігієни.
2. Типи хакерських атак у цифровому просторі.
3. Що таке інтернет-браузер та як його убезпечити?
4. Які загрози існують в месенджерах для користувачів та чи можливо повністю захистити приватне листування?
5. Основні загрози безпеки у соціальних мережах.
6. Чи можливо повністю контролювати свої дані та приватність у соцмережах?

Завдання для самостійної роботи



Ситуаційні завдання:

1. Уявіть, що хакери здійснили атаку на сайт Вашого навчального закладу і змінили головну сторінку. Які дії Ви виконатаєте в такому випадку?
2. Ви підозрюєте, що хтось отримав несанкціонований доступ до особистих даних Ваших здобувачів освіти. Які кроки необхідно зробити для мінімізації наслідків?
3. Уявіть, що Ви отримали листа від технічної підтримки з проханням надіслати логін та пароль. Чи варто реагувати на таке звернення і чому?
4. Ваш колега користується одним паролем для всіх онлайн-сервісів. Чому це небезпечно і які поради Ви можете дати йому?
5. Під час онлайн-уроку до Вас приєдналися невідомі особи і почали писати нецензурні слова. Як запобігти таким ситуаціям надалі?
6. Ваш колега по роботі повідомив, що його обліковий запис у соцмережі було зламано. Які рекомендації Ви можете дати щодо подальших дій у такому випадку?
7. Під час роботи в Інтернеті раптом перестали відкриватися всі сайти і з'явилося вікно з вимогою викупу. Що сталося і що робити у такій ситуації?

Матеріал для опрацювання

1. Поняття кібергігієни.

З кожним пройденим днем використання інформаційних технологій все ширше впливає на повсякденне життя людей у сучасному світі. Сьогодні, майже у кожного є смартфон з можливістю доступу до Інтернет-мережі, що дозволяє користувачам завжди залишатися на зв'язку. Зокрема, в будь-який момент можна перевірити електронну пошту чи месенджер, придбати квиток на кіно або забронювати житло для відпустки, а також здійснювати фінансові операції, не виходячи з дому. Усі ці дії в Інтернеті включають обмін певною особистою інформацією або конфіденційними даними, які, при необережному використанні, можуть потрапити в руки зловмисників.

Необхідним елементом цифрового життя є кібергігієна, оскільки вона допомагає забезпечувати захист даних та інформації в інтернеті. Розвиток технологій дозволяє легко отримувати доступ до різних сервісів та даних, але це також збільшує нашу вразливість перед кіберзлочинцями. Тому важливо дотримуватися правил та практик кібергігієни.

Кібергігієна важлива тоді, коли ми тримаємо телефон у руках та ділимося особистою інформацією в соціальних мережах, відповідаємо на повідомлення від незнайомців чи не помічаємо незвичайної поведінки друзів онлайн. Справжній захист вимагає такого ж уважного ставлення до дій в мережі, як і офлайн. Хоча кіберзлочинець не може завдати фізичної шкоди, його хитрість може використати вашу необережність для отримання ваших

даних або грошей. Таким чином, правила кібергігієни є своєрідними манерами та навичками самозахисту у цифровому середовищі. Важливо популяризувати цю ідею серед широкого загалу.

Кібергігієна використовується для забезпечення безпеки особистої, фінансової та іншої інформації під час користування комп'ютером чи мобільним пристроєм. Ефективна кібергігієна передбачає виконання щоденних практик забезпечення інформаційної безпеки в Інтернеті. Це охоплює не лише регулярне оновлення програмного забезпечення браузера, встановлення та підтримку захисного програмного забезпечення, вибір надійних паролів та їх конфіденційність, але й уникання використання відкритих мереж Wi-Fi для банківських операцій та інших фінансових транзакцій. Головна мета – блокування шахраїв і зловмисників.

Потенційні загрози для безпеки в Інтернеті включають:

- Вторгнення шкідливого програмного забезпечення в інформаційну систему: віруси, троянські програми, мережеві хробаки, програми-шпигуни, рекламні системи.
- Хакерські атаки.
- Мережа BotNet – це група комп'ютерів, на яких запущено боти – автономне програмне забезпечення.
- DDoS-атаки (розподілена атака на відмову в обслуговуванні) – спроба зробити ресурси комп'ютерної системи недоступними для користувачів.
- Фішинг – вид обману, мета якого полягає в виманюванні особистих даних у користувачів онлайн-платформ, сервісів для обміну валюти, інтернет-магазинів і т.д.

Для смартфонів існують ті самі загрози, що і для стаціонарних комп'ютерів: віруси, троянські програми, мережеві хробаки, рекламні модулі тощо, спрямовані на різні типи мобільних пристроїв.

Ось кілька порад, які можна запам'ятати для забезпечення кібергігієни:

- Створюйте складні паролі та змінюйте їх регулярно.
- Утримуйте особисті дані від незнайомців.
- Використовуйте антивірусні програми та регулярно оновлюйте їх.
- Будьте обережні зі сторонніми застосунками та програмами, які завантажуєте на свій пристрій.
- Уникайте відкривання підозрілих листів, повідомлень чи посилань.

2. *Хакерські атаки.*

Хакерська атака (кібератака) – зловмисні дії з метою викрасти інформацію, котра зберігається в електронному виді, встановити контроль над чужою комп'ютерною системою та вивести комп'ютери з ладу.

Характерна особливість кібератак полягає у негайності їх виконання (протягом секунд, хвилин).

Об'єктами хакерських атак можуть бути як комп'ютерні системи в цілому (з урахуванням їхньої нормальної функціональності), так і їхні складові частини: інформаційні ресурси, дані, що передаються через канали зв'язку, програмні та технічні засоби та інше.

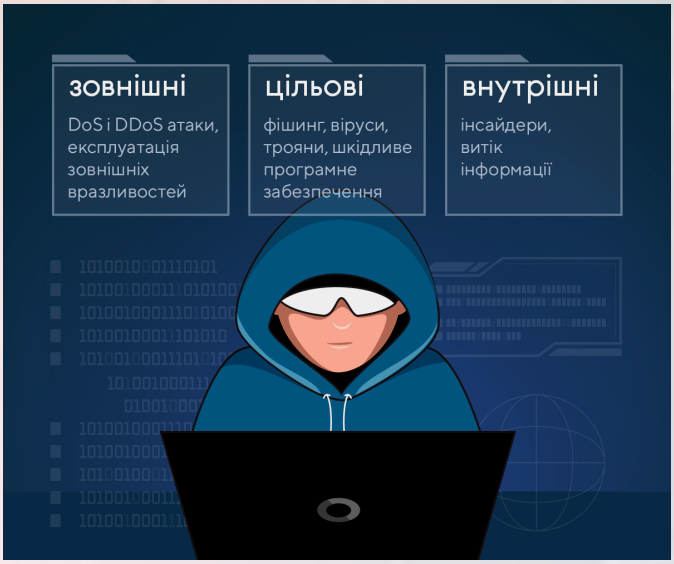
Існують три основних типи кібератак, спрямованих впливати на об'єкти:

1. Порушення конфіденційності – завданням атаки є отримання несанкціонованого доступу до інформації.

2. Порушення цілісності – передбачає несанкціоновану зміну інформації або програмних та технічних засобів системи.

3. Порушення доступності – метою атаки є дестабілізація роботи системи через створення перешкод для легітимних користувачів у доступі до системи або необхідних для вирішення функціональних завдань даних.

До найпоширеніших видів атак належать:



1. *Відмова в обслуговуванні* (атака DoS) – мережева атака, яка полягає в перенавантаженні компонентів комп'ютерних систем, що призводить до блокування доступу авторизованих користувачів до ресурсу чи комп'ютера.

2. *Фішинг* – атака з використанням технічних та соціально-інженерних методів для введення в оману авторизованих користувачів та намагання їх розкрити особисті дані за допомогою створення копій сайтів та повідомлень, схожих на легальні та відомі користувачам.

3. *Віруси та трояни* (Malware) – введення шкідливого програмного забезпечення в комп'ютер, яке може пошкоджувати, змінювати чи знищувати інформацію, а також впливати на працездатність операційної системи.

4. *Вимагання викупу* (Ransomware) – запуск шкідливого програмного забезпечення, яке шифрує дані чи робить їх копії для подальшого шантажу власника цих даних з метою отримання викупу.

5. *Людина посередині* (Man-in-the-Middle) – мережева атака, яка полягає в додаванні стороннього користувача до існуючого каналу зв'язку між двома системами для отримання доступу до всієї передаваної інформації та можливості її підміни.

6. *Експлойт на невідому вразливість* (Zero-day exploit) – атака на невідомі розробнику вразливі місця ліцензійного програмного забезпечення без спеціальної системи захисту.

7. *Міжсайтовий скриптінг* (XSS) – атака на безпечні сайти через додавання небезпечного коду, що може передавати дані користувача хакерам.

8. *Логічні бомби* (Logic bombs) – атака за допомогою легальних програм, до яких додається шкідливий код, що виконується за певних умов, визначених хакером.

Незалежно від складності систем захисту повністю уникнути кібератак неможливо. Проте підтримка функціонування таких систем та постійний моніторинг і своєчасне виявлення вразливих місць дозволяють знизити ризики та наслідки хакерських атак, а також допомагають фахівцям у вдосконаленні системи.

Найбільші жертви кібератак за 2022 та 2023 роки

Жертва кібератаки	Наслідки
Twitter	викрадено особисту інформацію про 5,4 мільйона користувачів
Червоний Хрест	викрадено особисту інформацію про 515 тисяч людей, включаючи їхню локацію
Міністерство національної оборони Португалії	викрадено конфіденційні документи НАТО
Сайти аеропортів	зламано сайти 23 аеропортів США, Японії, Естонії та Литви

3. Безпечний веб-браузер.

Веб-браузер – це програмне забезпечення, яке дозволяє користувачам отримувати інформацію з веб-сайтів у мережі Інтернет.

Браузери перекладають код веб-сторінок у зрозумілий для людини вигляд. Для передачі використовується протокол HTTP або його безпечніша версія HTTPS.

Протокол – це набір правил передачі файлів (тексту, зображень, відео тощо) через мережу Інтернет. Приклади браузерів: «Google Chrome», «Mozilla Firefox», «Microsoft Edge», «Apple Safari», «Internet Explorer».

Проте браузери на даний момент не тільки надають доступ до веб-сторінок, але також виступають платф ормою для додаткових програм, які полегшують використання Інтернету. Ці програми відомі як плагіни і розширюють функціональність браузера, додаючи нові можливості. Більшість плагінів можуть додавати додаткові панелі інструментів, інструменти пошуку та маркетингові помічники. Деякі плагіни працюють в фоновому режимі і залишаються непомітними для користувача, не маючи графічного інтерфейсу. Також існують потенційно шкідливі плагіни. Для того щоб запам’ятати користувача, браузери використовують файли, відомі як cookies.

Cookies – це невеликі текстові файли на комп’ютері, які зберігають інформацію про попередні взаємодії користувача з веб-сайтами.

Окрім збережених входів, вони можуть запам’ятовувати налаштування користувача, переглянуті товари, введений текст і багато іншого. Коли користувач робить дії на веб-сайті, такі як додавання товару в корзину, ця інформація записується в cookies і відправляється браузеру. Cookies можуть бути тимчасовими або постійними, залежно від

того, чи залишаються вони на комп'ютері після закриття вкладки. Розробники визначають, які саме cookies використовувати на своєму веб-сайті – тимчасові чи постійні.

Cookies самі по собі не є загрозливими, адже це всього лише звичайні текстові файли. Вони не здатні запускати процеси на вашому комп'ютері чи взаємодіяти з операційною системою. Проте існує можливість їх перехоплення або викрадення для відстеження ваших дій в мережі чи незаконного доступу до вашого акаунту.

Зазвичай інформацію, яку зберігають в cookies, шифрують перед передачею, а самі файли передаються за допомогою HTTPS-протоколу. Це сприяє захисту даних користувача, але відповідальність за впровадження шифрування та безпечну передачу лежить на розробнику веб-сайту. Користувач, з свого боку, може обмежити використання cookies браузером або періодично очищати їх самостійно. Відключення cookies взагалі є не завжди ефективним рішенням. Наприклад, багато інтернет-магазинів працюють виключно за допомогою cookies. Якщо ви забороните браузеру їх використовувати, сервер не зможе запам'ятати ваш кошик.

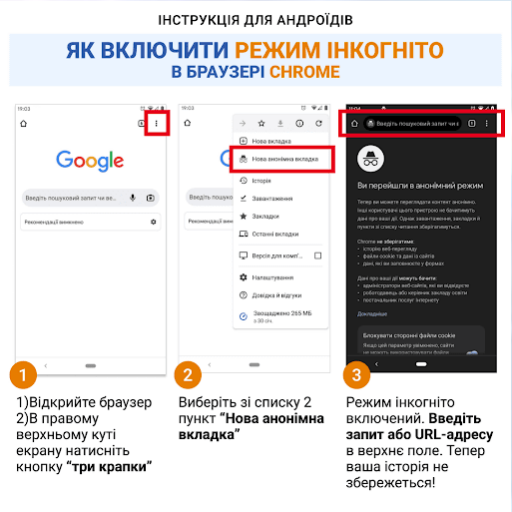
Чому браузери можуть становити загрозу безпеці?

- Браузери застарівають, і в них з'являються вразливості, якими можуть користуватися хакери здалеку.
- Хакери взламують легітимні сайти та вставляють у них шкідливий код та програми, і ви можете не знати, що вже стали жертвою
- Зловмисники втручаються в громадські точки доступу до Інтернету, намагаючись перехопити інформацію користувачів.

Слід зазначити, що новини про кібербезпеку часто повідомляють про те, що браузери регулярно оновлюються та публікують інформацію про виявлені та виправлені вразливості. Це пояснюється тим, що нові вразливості виявляються практично щодня, і хакери миттєво використовують їх у своїх атаках. Важливо розуміти, що не існує абсолютно безпечного браузера, і іноді вразливості можуть існувати протягом тривалого часу. Щоб уникнути потрапляння в неприємності, важливо дбайливо враховувати безпеку свого інтернет-оглядача. Варто мати на увазі, що ваша недбалість може призвести до ризиків не лише для вас особисто, але й для всієї вашої організації.

Як забезпечити безпеку свого браузера?

- Постійно оновлюйте програму перегляду веб-сторінок, щоб уникнути виявлення в ній відомих вразливостей.
- Дбайливо налаштовуйте параметри конфіденційності вашої інформації у браузері.
- Встановлюйте додаткові засоби безпеки, такі як HTTPS Everywhere (який попереджає про відсутність захисту HTTPS на сайті та можливий ризик перехоплення даних, таких як логіни, паролі і т. д.) або AdBlock (блокувальник реклами).



Необхідно розуміти, що ви несете відповідальність за безпеку не лише свого комп'ютера, а й за дані, якими ви володієте. Інформація, що знаходиться на вашій робочій станції, повинна бути захищена не лише за допомогою антивірусного захисту, але й за допомогою регулярних резервних копій та обмеженням доступу.

Щодо даних, які ви вводите на різних сайтах Інтернету під час реєстрації чи використання, запам'ятайте, що те, що ви відправляєте в мережу, вже не належить вам. Інформація може бути вкрадена, скомпрометована, підроблена або знищена навіть без вашого відома, не кажучи вже про дозвіл.

Рекомендуємо утримуватися від введення персональних даних (логіна, пароля, номера телефону чи платіжної картки) на запити неперевірених або підозрілих сайтів. Пам'ятайте, що сайт є підозрілим, якщо ви його бачите вперше!

Дані слід надавати лише тим ресурсам, які пройшли вашу перевірку або є відомими мережами (наприклад, «Google», «Facebook», «Rozetka», «Twitter» та інші). Також важливо перевіряти назву сайту в адресному рядку браузера (наприклад, www.rozetka.ua, а не rozetka.ug чи rozteka.com.ua).

Введення інформації з платіжних карток чи паролів слід здійснювати лише на сайтах з позначкою «замочка» в адресному рядку. Таке з'єднання вважається захищеним, і ваші дані не потрапляють до рук сторонніх осіб, які можуть отримати доступ до вашої комунікації з інтернет-сторінкою.

Щодо робочої адреси електронної пошти, телефону та іншої офіційної інформації, важливо не використовувати ці дані ніде, окрім офіційних джерел. Особливо не рекомендуємо використовувати робочі засоби комунікації, такі як номер телефону чи адреса електронної пошти, для особистих питань. Ризики використання цих даних надто великі, оскільки хакери активно полюють на них і використовують для спроб атак на різні установи.

4. Безпека месенджерів.

У перекладі із англійської мови термін «messenger» виражає ідею *«гонця», «посланника» або «представника»*. Це означає особу, яка приносить новини. Таким чином, що таке месенджери та які є їх характеристики?

У сфері інформаційних технологій термін ***«месенджер»*** давно закріпився як програмний засіб для миттєвого обміну короткими повідомленнями через електронні канали зв'язку. Зазвичай, це відбувається через Інтернет, але існують винятки.

Які можливі ризики використання месенджерів?

1. Розголошення особистої інформації: від номеру телефону до фотографій та іншого.

2. Шахрайство – шахраї часто використовують месенджери для ухилень від виявлення.

3. Розповсюдження шкідливого програмного забезпечення через функції автозавантаження.

У 2017 році була помічена тенденція викрадення інформації через месенджери. У 2018 році кількість витоків інформації через месенджери зросла на 14,3%, хоча раніше цей канал не вирізнявся в статистиці. Крім того, постійно виникають нові модифікації шкідливих програм, які відстежують переписку у популярних месенджерах, таких як «Telegram», «WhatsApp», «Skype» та інші.

Люди все частіше діляться особистою інформацією в мобільних додатках. Якщо п’ять років тому можна було втратити лише особисті фотографії, то сьогодні це може бути комерційна переписка, банківські рахунки, контакти. Розробники додатків часто не встигають за хакерами, тому дотримання правил безпеки може допомогти вам у забезпеченні особистої безпеки.

Як захистити себе під час користування месенджерами?

1. Не передавайте через месенджер жодну інформацію, розголошення якої вам небажане.

2. Вимикайте автоматичне завантаження файлів, особливо для контактів, які не входять до вашої адресної книги.

3. Утримуйтеся від переходу за посиланнями, особливо скороченими, надісланими недовіреними контактами.

4. Постійно оновлюйте месенджери.

Пам’ятайте головне: ваша особиста безпека – це ваша відповідальність. Але від неї може залежати добробут та майбутнє не тільки для вас, а й для інших громадян України.

5. *Безпека соціальних мереж.*

Соціальні мережі, такі як Facebook, LinkedIn, Instagram чи Snapchat, дають можливість спілкуватися з друзями, партнерами та колегами по всьому світу, ділитися особистою інформацією. Проте варто пам’ятати, що це несе певні ризики. Хакери можуть дізнатися, де ви перебуваєте, чим займаєтеся, що вам належить та інші конфіденційні дані. Безпека та соцмережі не завжди сумісні речі. Реєструючись, користувачі фактично розкривають інформацію, яку можна використати в комерційних цілях – фото, музичні уподобання, підписки. Усе це – елементи «профайлу», за якими нас знайдуть не лише друзі, а й маркетологи. Тож особисті дані можуть бути продані. Багато власників сервісів за гроші віддадуть не лише інформацію про товари, які ви шукали, а й більшість особистих даних. Отож конфіденційну інформацію краще не завантажувати в соцмережі взагалі – ні в закриті альбоми, ні в особисті повідомлення.

У 2018 році Cambridge Analytica зібрала через свій додаток у Facebook дані користувачів і використала їх для політичної реклами, зокрема під час виборів у США та референдуму про Brexit. Це торкнулося 87 млн осіб. Компанія заперечувала провину, але збанкрутувала. Засновник Facebook визнав помилку і соцмережу оштрафували на $5 млрд. Отож, щоб убезпечити себе, не варто ділитися конфіденційною інформацією в соцмережах.

Реєструючись в соціальних мережах, ви можете обрати будь-яке ім’я, а не обов’язково справжнє. Надавайте лише мінімум даних, необхідних для реєстрації. Використовуйте окрему електронну пошту і не вказуйте свій номер телефону, щоб захистити конфіденційність. Обережно підбирайте фото профілю та інші зображення. Вони можуть містити метадані про час і місце зйомки. Також перевірте, чи немає на фото сторонніх об’єктів, які розкриють особисту інформацію. Не відповідайте правдиво на контрольні запитання для відновлення пароля. Ці дані можна знайти в інших мережах. Вигадайте власні відповіді і збережіть їх окремо, щоб не забути.

Забезпечте безпеку свого облікового запису надійним паролем. Ефективні паролі мають велику довжину, складність і унікальність. Це означає, що вони повинні містити від

10 до 16 символів, включати різні типи символів (букви, цифри, спеціальні знаки) і відрізнятися для кожного облікового запису та системи. Уникайте паролів, які базуються на простих словах, що можна знайти в словниках. Уникайте використання особистих даних, таких як дата народження, ім’я близької особи, інформація про вас, що доступна в обліковому записі.

Рекомендується використовувати парольні фрази для уникнення проблем зі слабкими паролями. Виберіть фразу, яку ви не зможете легко забути в наступні 2-3 дні: фрагмент вірша чи пісні, прислів’я, гасло тощо. Потім перетворіть цю фразу в унікальне "слово", прибравши пробіли та замінивши деякі літери на цифри або спеціальні символи.

Ніхто, окрім вас, не повинен знати ваші паролі та парольні фрази. Не розголошуйте їх нікому, навіть близьким особам. Ніколи не залишайте ваші паролі та парольні фрази на папері або в незашифрованому файлі. Використовуйте надійні парольні менеджери, такі як 1Password (платний), Bitwarden (безкоштовний), Dashlane (безкоштовний з обмеженнями), або KeePassXC (безкоштовний).

Регулярно змінюйте свої паролі та парольні фрази, принаймні один раз на рік. Паролі, які використовуються найчастіше, повинні бути змінювані принаймні щомісячно або раз на два місяці.

СЕМІНАРСЬКЕ ЗАНЯТТЯ 2

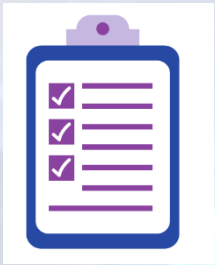
Тема: «Нормативно-правові засади забезпечення безпеки цифрового простору в ЗП(ПТ)О»

Мета: поглиблення розуміння слухачами нормативно-правових аспектів регулювання безпеки цифрового простору та захисту пресональних даних в освітньому середовищі, сприяння критичного мислення стосовно впровадження та дотримання заходів безпеки в електронному просторі, форування усвідомлення важливості забезпечення безпеки цифрового простору.

Основні поняття: цифровий простір, персональні дані, кібербулінг, електронна пошта, фішинг, освітня послуга, ЄДЕБЕО,

Уміння, які мають бути вироблені, та навички, які мають бути напрацьовані під час заняття: створювати та впроваджувати ефективні стратегії та політику забезпечення безпеки в електронному середовищі, визначати ситуації кібербулінгу, розуміти їхні наслідки та розробляти заходи для їх запобігання, ефективно застосовувати технічні та організаційні заходи для захисту особистої інформації та персональних даних, визначати потенційні загрози у вхідних повідомленнях, використовувати шифрування та інші засоби для безпеки електронного листування.

План



1. Захист персональних даних.
2. Дії закладу освіту для безпеки цифрового простору.
3. Кібербулінг як небезпека цифрового простору.
4. Безпека електронної пошти.

Питання для обговорення

1. Поняття персональні дані згідно чинного законодавства України? Яким чином ЗП(ПТ)О регулюють їх обробку?
2. Інструменти та методи реалізації кібербезпеки цифрового простору в ЗП(ПТ)О?
3. Правила безпечного користування електронною поштою.
4. Поняття кібербулінгу. Який порядок реагування ЗП(ПТ)О на кіберінциденти?
5. Поняття ліцензійного програмного забезпечення. Які правові наслідки передбачені за піратство у цифровому просторі?

Завдання для самостійної роботи

Ситуаційні завдання

1. Здобувач освіти поскаржився, що його обліковий запис у соцмережі використовують для кібербулінгу інших учасників освітнього процесу. Які дії ви виконаєте у такій ситуації?
2. Колега використовує піратське програмне забезпечення. Які аргументи можна навести, щоб переконати його відмовитися від цього?
3. Під час онлайн-уроку Ви помітили, що хтось знімає екран і транслює заняття без Вашого дозволу. Які правові наслідки може мати таке втручання?
4. Ви хочете розмістити на сайті навчального закладу фото здобувачів освіти. Чи потрібно для цього отримати згоду батьків згідно закону?

Матеріал для опрацювання

1. Захист персональних даних.

Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована[1].

Персональні дані здобувачів освіти включають особисті справи, медичні довідки, інформацію у друкованих або електронних класних журналах, щоденниках, відеозаписах із усною відповіддю учнів тощо. У законодавст ві відсутні чіткі межі щодо визначення, які дані можна вважати персональними. З метою належного проведення освітньої діяльності, забезпечення права на освіту та створення якісних і безпечних умов навчання заклад освіти має доступ до певних персональних даних учнів, їхніх батьків і педагогічних працівників. Заклад освіти має право виконувати різні операції з цими даними, такі як збір, реєстрація, накопичення, зберігання, адаптація, зміна, оновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлювання та знищення персональних даних. Всі дії з обробки персональних даних регулюються статтею 2 Закону України «Про захист персональних даних».

Учасники освітнього процесу, включаючи учнів, батьків і педагогічних працівників, є суб'єктами персональних даних, тобто особами, чиї дані обробляються. Заклад освіти і його педагогічний персонал несуть відповідальність за збереження цих даних. Використання персональних даних здобувачів освіти допускається лише в професійних цілях. Наприклад, якщо оцінки здобувачів публікуються у відкритому доступі, вони повинні бути знеособлені. Аналогічно, якщо зведений облік результатів навчання розповсюджується, він також повинен бути знеособлений.

Обробка персональних даних здійснюється відповідно до законодавства. Перелік персональних даних не є вичерпним, оскільки це різноманітна інформація, за допомогою

[1] стаття 2 Закону України «Про захист персональних даних» https://bit.ly/3kl6uY8

якої можна ідентифікувати особу, зокрема за її ПІБ, паспортними даними та облікової картки платника податків.

Правові підстави обробки персональних даних у сфері освіти[2]:

1) згода суб'єкта персональних даних на обробку його персональних даних;

2) дозвіл на обробку персональних даних, що надається власнику персональних даних відповідно до закону виключно для виконання його повноважень;

3) укладення та виконання правочину, у якому бере участь суб'єкт персональних даних;

4) захист життєво важливих інтересів суб'єкта персональних даних;

5) виконання обов'язків власника персональних даних, передбачених законом;

6) захист законних інтересів власника персональних даних або третьої особи, якій передаються персональні дані.

У сфері освіти підставами для обробки персональних даних є:

- дозвіл на обробку персональних даних, отриманий від володільця персональних даних згідно з законом для виконання його повноважень;
- виконання обов'язків власника персональних даних, передбачених законом.

Освітня послуга – це комплекс дій суб'єкта освітньої діяльності, спрямованих на досягнення здобувачем освіти очікуваних результатів навчання[3].

Заклади освіти надають освітні послуги, а здобувачі їх отримують. Оскільки отримання освітньої послуги передбачає зарахування до закладу освіти, батьки або здобувачі освіти подають заяву, документи та/або укладають договір. Зарахування до закладу освіти здійснюється на підставі відповідної заяви та наданих персональних даних. Дозвіл, наданий батьками або повнолітніми здобувачами освіти, є ще однією підставою для обробки персональних даних у закладі освіти для виконання його повноважень. З цього випливає додаткова підстава виконання обов'язку власника персональних даних, який передбачений законами у сфері освіти.

Деякі навчальні заклади перейшли на зберігання ділової документації у електронному форматі. *Перелік особистих даних здобувачів освіти*, які обробляються у електронній системі управління навчальним процесом, включає:

- ПІБ учня;
- дата народження.;
- стать;
- дані документа, що посвідчує особу;
- інформація про навчальний заклад та клас/групу здобувача освіти;
- інформація про пільгові категорії, якщо такі є.

Крім того, система також містить інші дані щодо здобувачів, такі як:

- відвідування та пропуски занять;
- результати оцінювання (поточні, тематичні, підсумкові);
- теми уроків.

Також у системі зберігаються *особисті дані батьків неповнолітніх здобувачів освіти*, зокрема:

- ПІБ батьків;

---

[2] Відповідно до статті 11 Закону України «Про захист персональних даних»

[3] Згідно зі статтею 1 Закону України «Про освіту» (посилання)

- інформація про пільгові категорії здобувача, якщо такі є;
- контактна інформація.

Особисті справи здобувачів освіти містять такі дані:

- номер особової справи;
- інформація про навчальний заклад;
- адреса закладу освіти;
- ПІБ директора навчального закладу;
- інформація про здобувача освіти;
- дані про місце проживання здбувача;
- інформація про батьків або осіб, що їх замінюють;
- дані про попередній навчальний заклад (якщо є);
- відомості про перехід з одного закладу освіти до іншого (якщо є) та інше.

На сьогоднішній день існують два державних електронних реєстри освіти, в які заносяться персональні дані освітян:

1. Єдина державна електронна база освіти (ЄДЕБО)
2. Автоматизований інформаційний комплекс освітнього менеджменту (АІКОМ)

Єдина державна електронна база освіти (ЄДЕБО) – це автоматизована система, яка збирає, обробляє, зберігає та захищає інформацію про освітян, учасників освітньої діяльності. Вона створюється та використовується для задоволення потреб фізичних та юридичних осіб та є необхідною складовою освітньої інфраструктури[4].

Держава є власником ЄДЕБО та має виключні майнові права на її програмне забезпечення. Міністерство освіти і науки України є розпорядником та власником інформації в ЄДЕБО, а технічний адміністратор – державне підприємство «Інфоресурс», що входить до сфери управління розпорядника ЄДЕБО.

ЄДЕБО включає такі компоненти:

- реєстр учасників освітньої діяльності;
- реєстр освітян;
- реєстр документів про освіту;
- реєстр сертифікатів зовнішнього незалежного оцінювання;
- реєстр студентських (учнівських) квитків;
- реєстр педагогічних та науково-педагогічних працівників;
- реєстр сертифікатів педагогічних працівників

Головна мета функціонування ЄДЕБО:

– збір, реєстрація та облік інформації для видачі документів в сферах загальної середньої, професійної, фахової передвищої, вищої освіти та освіти дорослих;
– супроводження прийому на навчання у заклади освіти згідно з законодавством;
– електронний вступ – можливість подання заяв про допуск до участі в конкурсному відборі через Інтернет;

[4] Згідно зі статтею 74 Закону України «Про освіту» (посилання)

– формування рейтингових списків вступників та списків рекомендованих для зарахування до закладів освіти.

Захист інформації в ЄДЕБО здійснюється через створення комплексної системи захисту інформації з підтвердженою відповідністю, відповідно до вимог законодавства у сфері захисту інформації, що перебуває у власності держави[5].

Припинення обробки персональних даних здобувачів освіти у державних реєстрах ЄДЕБО та АІКОМ призводить до неможливості:

- здійснення навчання здобувачів освіти;
- видачі їм документів про освіту;
- перерахування коштів державних субвенцій для навчання учня в закладі освіти;
- замовлення та отримання підручників для дитини.

2. Дії закладу освіти для безпеки цифрового простору.

Міжнародний союз електрозв'язку визначає наступні рекомендації для закладів освіти. Заклад освіти має:

- ✓ забезпечити захищену та надійну мережу, а для цього потрібно використовувати послуги офіційного інтернет-провайдера;
- ✓ використовувати програмне забезпечення для фільтрації та моніторингу безпеки пристроїв;
- ✓ встановлювати в межах освітнього закладу політику, яка визначає, де і як можуть використовувати технології різні учасники навчального процесу, а також порядок реагування на інциденти, пов'язані з безпекою здобувачів освіти, зокрема, в цифровому середовищі;
- ✓ організовувати для здобувачів освіти навчання з питань цифрової безпеки;
- ✓ забезпечувати достатній рівень підготовки всіх працівників (зокрема, технічного персоналу), а також регулярне підвищення їхньої кваліфікації;
- ✓ призначити у закладі освіти спеціального координатора і створити можливості для обліку та реєстрації інцидентів, пов'язаних з цифровою безпекою, щоб сформувати цілісне уявлення про наявні у закладі освіти проблеми та тенденції, що вимагають уваги;
- ✓ вжити заходів для того, щоб адміністративно-управлінський персонал та керівники були достатньо обізнані в питаннях цифрової безпеки у закладі освіти;
- ✓ враховувати потенційний вплив Інтернету та цифрових технологій на навчання та психіку здобувачів освіти.

Міністерство освіти наголошує на важливості того, щоб педагоги вибирали для здійснення навчання одну або дві освітні платформи. Це сприятиме полегшенню організації навчання для здобуачів освіти, педагогів та батьків. Також використання мінімальної кількості платформ, необхідної для забезпечення освітнього процесу, робить навчання більш безпечним, оскільки це зменшує ризик витоку особистих даних.

Якщо мова йде про вибір провайдера, рекомендується обирати перевірені платформи від офіційних виробників і утримуватися від надання зайвих персональних даних здобувачів освіти і викладачів для користування платформами. Заклад освіти повинен

[5] Згідно з «Положенням про Єдину державну електронну базу освіти» (посилання)

повідомити учнів та батьків про те, які персональні дані будуть оброблятися при використанні певної платформи навчання.

Одночасно закладам освіти слід звернути увагу на розробку конкретних правил поведінки та безпеки в цифровому середовищі, а також встановити порядок реагування на інциденти. Спільне обговорення та ухвалення цих правил з усіма учасниками освітнього процесу допоможе мінімізувати неприємні випадки, які можуть виникати під час дистанційного навчання.

3. Кібербелінг як небезпека цифрового простору.

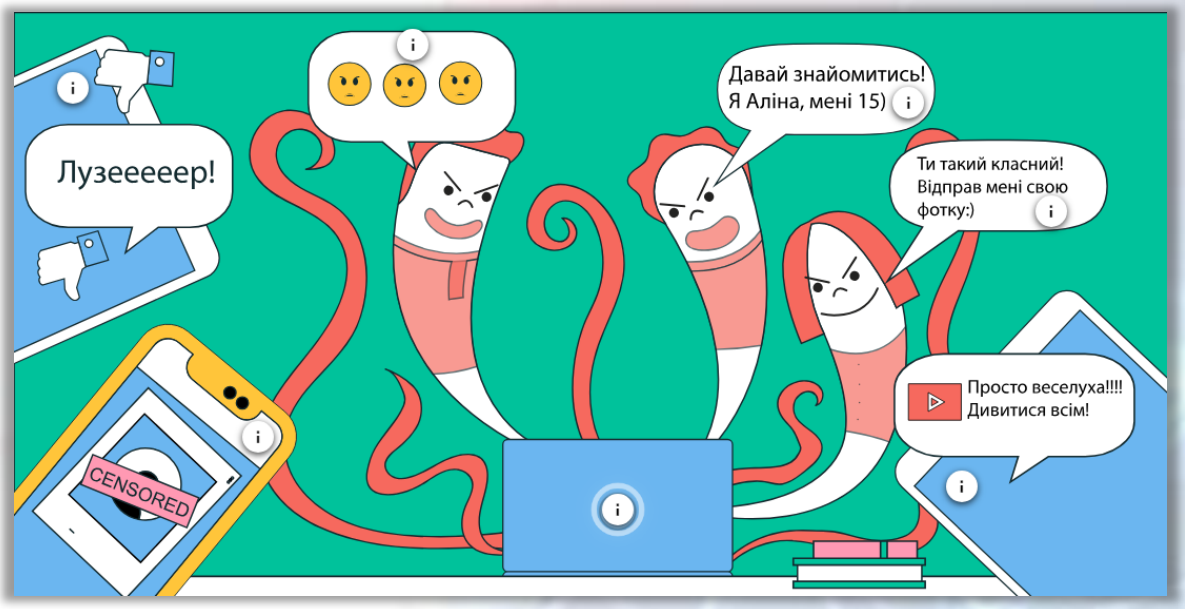
Окрім відомих загроз, які чекають нас в Інтернеті (віруси, спам, шахрайство, фішинг/злам особистих сторінок), існують небезпеки, які завдають не тільки матеріально-технічної, а й психологічної та певного роду фізичної шкоди кожній людині.

Кібербулінг – це умисне домагання людиною або групою людей конкретної особи у мережі Інтернет, як правило, тривало.

Відмінності між кібербулінгом та булінгом обумовлені особливостями Інтернет-середовища, такими як анонімність, можливість підміни ідентичності, здатність охоплювати велику аудиторію одночасно (особливо ефективно для поширення пліток) та можливість тероризувати та утримувати жертву у напрузі будь-де і будь-коли.

Мета кібербулінгу різниться в залежності від його форми, проте в будь-якому випадку вона пов'язана із завданням шкоди іншій людині – насамперед психологічної, але шкода може бути і матеріальною або фізичною, якщо насильство з онлайн-середовища перейде у реальну площину.

Кібербулінг може проявлятися у наступних формах:



Детальне ознайомлення з інтерактивною інфографікою див. тут

ВІДСКАНУЙ МЕНЕ

Кібербулінг є формою психологічного насильства. Види кібербулінгу включають:

1. Віртуальна перепалка (флеймінг): обмін короткими гнівними репліками між учасниками за допомогою комунікаційних технологій, зазвичай на форумах та в чатах.

2. Нападки (домагання): регулярні образливі висловлювання на адресу жертви через СМС, телефонні дзвінки тощо, що перевантажують особисті канали комунікації.

3. Наклеп: поширення неправдивої та принизливої інформації.

4. Самозванство: використання особистих даних жертви (логіни, паролі) для негативної комунікації в її ім'я.

5. Публічне розголошення особистої інформації: поширення особистих даних з метою образи чи шантажу.

6. Ошуканство: виманювання конфіденційної інформації для власних цілей або передачі іншим особам.

7. Відчуження (острокізм, ізоляція): онлайн відчуження через захист паролів, формування списків небажаної пошти або друзів.

8. Кіберпереслідування: приховане відстеження жертви для скоєння фізичних нападів чи сексуальних злочинів.

9. Хепіслепінг: реальні напади, які записуються на відео для розміщення в Інтернеті та можуть призвести до летальних наслідків.

10. Онлайн-грумінг: будування довірливих відносин з дитиною з метою отримання її інтимних фото/відео та подальшого шантажування.

Ознаки кібербулінгу:

- систематичне (повторюване) здійснення дій;
- наявність учасників – кривдника (булера), потерпілого (жертви булінгу), спостерігачів (при наявності);
- дії або бездіяльність кривдника, які призводять до завдання психічної та/або фізичної шкоди, приниження, страху, тривоги, підпорядкування інтересам кривдника та/або спричинення соціальної ізоляції потерпілого.

Якщо висловлювання, поширення зображень тощо в інтернеті стосовно конкретної особи розглядається нею як жарт, не має систематичного характеру та не викликає негативних емоційних реакцій, такі дії не можна вважати кібербулінгом.

Сторони кібербулінгу та їхні ролі

Кривдник (булер) – учасник освітнього процесу, включаючи малолітніх або неповнолітніх осіб, які здійснюють булінг (цькування) стосовно іншого учасника освітнього процесу.

Потерпілий (жертва) – учасник освітнього процесу, включаючи малолітніх або неповнолітніх осіб, який став об'єктом булінгу (цькування).

Спостерігач – свідки та (або) безпосередні очевидці випадку булінгу (цькування).

Коли кібербулінг має місце в Інтернеті, може здатися, що вас атакують скрізь, навіть у вашому власному будинку. Здається, що виходу немає. Негативні наслідки можуть тривати довгий час і впливати на людину різними способами:

Ментально – почуття смутку, пригніченості, навіть гніву, відчуття безвихідності.

Емоційно – почуття сорому, втрата інтересу до того, що вам подобається.

Фізично – відчуття втоми (втрата сну) або такі симптоми, як біль у животі та головний біль.

Переживання того, що з вами насміхаються або вас переслідують, може заважати людям висловлювати свої думки або намагатися вирішити проблему. У найгірших випадках кібербулінг може призвести навіть до скоєння самогубства.

Кібербулінг може впливати на нас різними способами. Проте з цим можна боротися, і люди можуть повернути впевненість у собі та здоров'я.

4. Безпека електронної пошти

Кожен день ми використовуємо електронну пошту як для робочих, так і для особистих цілей. Вона стала ключовим каналом зв'язку з нами і, таким чином, є особливо привабливою для кіберзлочинців та інших зацікавлених сторін. Сьогодні ми розглянемо потенційні загрози під час використання електронної пошти і обговоримо заходи, які можна прийняти для власного захисту.

Після того, як люди почали активно використовувати електронну пошту, історія зафіксувала безліч успішних кібератак, де електронна пошта слугувала інструментом для поширення шкідливого програмного забезпечення та виманення конфіденційної інформації. Згідно з дослідженнями, 37% усіх кібератак здійснюються через електронну пошту.

Електронна пошта притягує кіберзлочинців через легко доступність баз даних поштових скриньок в Інтернеті. Функція додатків до листів дозволяє злочинцям відправляти файли з шкідливим програмним кодом, а користувачі не завжди очікують отримати листи зі шкідливим вмістом і часто несвідомо відкривають всі вхідні листи. Злочинці використовують людську психологію, маскуючись під різні привабливі аспекти.

Перше правило безпеки електронної пошти – чітке розмежування особистого та службового акаунтів.

Службова пошта підтверджує вашу належність до організації (наприклад, vasyl@me.gov.ua), що викликає довіру до листів з цієї адреси. Дані зберігаються на серверах вашої установи, адмініструються відділом інформаційних технологій, і треті сторони не повинні мати доступ до цих даних.

Особиста пошта зберігається на серверах компанії, яка надає послуги поштового сервісу та містить вашу приватну інформацію, використовується для реєстрації в соціальних мережах та на інших ресурсах.

Які загрози появлюються під час використання поштової скриньки?

Фішинг – це схема, при якій хакери використовують підступи, щоб змусити користувачів передавати конфіденційну інформацію, таку як паролі та номери соціального страхування.

Зазвичай цей вид атаки включає надсилання спам-повідомлень, які виглядають як листи від довірених джерел, наприклад, банків (це нажива). В листі міститься посилання на фальшивий вебсайт, що схожий на довірене джерело (це пастка). Користувач, не підозрюючи нічого, вводить конфіденційну інформацію, вважаючи, що перебуває на безпечному сайті.

Мотиви зловмисників для відправки таких листів:

1. Зловмисник може використовувати листи з темою «Вас зламали! Швидше змініть пароль», видаючи себе за авторитетне джерело, наприклад, «Google». Це призводить до

того, що користувачі переходять за посиланням та вводять свої дані, які потім використовуються для доступу до їх облікових записів.

2. Ще однією загрозою є відправка листів з метою зараження системи або мережі організації, наприклад, через відправку шкідливих файлів. Після відкриття такого файлу відбувається шифрування комп'ютера з метою вимагання грошового викупу.

3. Також існує загроза отримання віддаленого доступу до комп'ютера та мережі. Наприклад, хакери можуть відправити електронний лист, видаючи себе за легітимне джерело, а при відкритті файлу відбувається зараження комп'ютера, що надає хакерам віддалений доступ для управління системою.

Давайте розглянемо, як розрізняти легітимні листи від фішингових. Ви отримали лист. Чекали на нього? Ні? Проведемо аналіз метаданих.

Аналіз метаданих:

1. Спочатку перевіримо, хто відправник. Ви його знаєте? Пам'ятайте, ім'я відправника може бути будь-яким.

2. Яка тематика повідомлення? Якщо вона викликає квапливість або закликає до швидкої дії, це може бути індикатором, що лист вимагає уваги та обережності. Наприклад: «Вас зламали! Швидше змініть пароль».

3. При відкритті листа зверніть увагу на правильність написання домену відправника. Кіберзлочинці часто підмінюють літери/символи, щоб залишитись непоміченими. Наприклад, «accounts-google.com» може маскуватися під «accounts.google.com». Якщо адреса виявилася достовірною, переходимо до аналізу змісту.

Аналіз змісту повідомлення:

1. Зверніть увагу, чи до Вас звертаються особисто за іменем, чи використовують загальні фрази «Шановні колеги», «Шановний клієнте» і т.д. Вказівка: якщо ім'я вказано, це може свідчити про спрямованість атаки саме на вас.

2. Інший індикатор фішингу – мова та наявність граматичних/орфографічних помилок. Наприклад, якщо ваш інтерфейс українською, а лист прийшов російською, це варто розглядати як підозріле.

3. Отримавши файл та пароль для його відкриття, будьте обережні. Це може бути підозріле явище, оскільки злочинці використовують архіватори для шифрування вмісту та ухилення від виявлення вірусів антивірусами.

4. Перевірте активні посилання у листі. Наведіть мишкою (без натискання) та перевірте, куди вас веде посилання. Переходимо до аналізу додатку.

Аналіз додатку:

Погляньте на розширення файлу. Деякі розширення можуть виконувати код на комп'ютері, що робить їх небезпечними:

1. Виконувані файли: EXE, COM, CMD, BAT, PS1, SWF, JAR, JS, VBS тощо.

2. Документи MS Office, особливо з макросами: DOC/DOCX/DOCM, XLS/XSLX/XLSM тощо.

3. PDF-документи: PDF.

4. Файли векторної графіки з вбудованим кодом: SVG.

5. Архіви файлів, особливо ті, що захищені паролем.

Таким чином, залишаючись уважними до цих ознак, ми можемо ефективно розрізняти легітимні листи від потенційно небезпечних фішингових спроб.

Рекомендації по убезпеченню електронної пошти

1. Складний пароль. Використовуйте пароль, що складається з літер, символів та цифр, і має довжину не менше 8 символів. Уникайте використання слів, які можна знайти у словнику. Приклади:

- Поганий пароль: rockandroll123
- Надійний пароль: T@8l3S0bk4hA7

2. Встановіть двофакторну аутентифікації на всіх платформах: другий фактор аутентифікації забезпечує додатковий рівень захисту.

3. Ніколи не відкривайте файли, не переконавшись у їхньому походженні. Використовуйте додаткові канали комунікації для перевірки листів, наприклад, телефон, месенджер і т.д.

4. Не використовуйте службову пошту в особистих цілях.

5. Якщо маєте сумніви щодо походження файлу, скористайтеся https://virustotal.com для сканування файлу за допомогою 50 антивірусних програм. Звертаємо увагу, що передаючи файл туди, ви може дати доступ до нього третім особам.

6. Вийдіть зі свого облікового запису після використання.

7. *Якщо у листі є скорочені посилання* (https://bit.ly/xxxxx), перевіряйте їх за допомогою таких сервісів:

- http://checkshorturl.com/
- http://www.expandurl.net/

САМОСТІЙНА РОБОТА

Тема: «Формування культури кібербезпеки в освітньому середовищі»

Мета: дослідження та розробка стратегії формування культури кібербезпеки в освітньому середовищі, зосереджена на розвитку учасників освітнього процесу у галузі понять культури кібербезпеки, використання правил цифрової гігієни та етики, розвитку критичного мислення та медіаграмотності для ефективної оцінки кіберризиків, вивчення методів розпізнавання фейків та аналізу поштових повідомлень.

Основні поняття: культура кібербезпеки, кібергігієна, медіаграмотність, фейки

Уміння, які мають бути вироблені, та навички, які мають бути напрацьовані під час заняття: оцінювати рівень кібербезпеки в різних ситуаціях, безпечне користування інтернетом та цифровими засобами, здатність відрізняти достовірну інформацію від фейків, аналізувати та оцінювати ризики в інтернет-середовищі, критично оцінювати медійні матеріали та визначати їхню достовірність

Завдання для самостійної роботи

1. Визначте свій рівень захисту персональних даних

Перейдіть за посиланням і дізнайтесь про свій рівень захисту персональних даних: посилання

ВІДСКАНУЙТЕ

2. Творче завдання

Створіть пам’ятку або інфографіку, де ви визначите основні правила цифрової гігієни та етики для користувачів освітнього середовища. Включіть поради щодо безпеки паролів, обмеження обміну особистою інформацією та інші важливі аспекти.

3. Ситуаційне завдання

1. **Які дії будуть найбільш ефективними в такій ситуації?** Ви отримали повідомлення від сторінки банку у соціальній мережі: «Треба відновити Ваші персональні дані, аби переконатися, що Ваша банківська картка не була вкрадена. Перейдіть за цим посиланням ...».

   а. перейду за посиланням та надам усю необхідну інформацію, адже це моя картка;
   б. проігнорую таке повідомлення;
   в. перевірю інформацію, наприклад, зателефонувавши до банку;
   г. усі відповіді правильні.

2. Вам в особисті повідомлення в Instagram прийшло повідомлення від друга/подруги: «*Привіт! Позич, будь ласка, гроші до завтра! Дуже треба!*» **Ваші дії?**

а. попросити написати номер картки для переказу та надіслати кошти;
б. зателефонувати другу/подрузі і запитати, чи це повідомлення від нього/неї;
в. зателефонувати другу/подрузі і запитати те, що може знати тільки він/вона;
г. усі відповіді правильні.

4. Практичне завдання

1. Давайте розберемося детальніше, якими бувають фейки. Прочитайте види фейків у стовпчику зліва та знайдіть до кожного виду його пояснення з правого стовпчика

1. фейкові журналістські матеріали	а) інформація, що була оброблена в графічних редакторах таким чином, щоб викривити події
2.фейкові пости	б) інформація, замаскована під новини, статті аналітику тощо
3. відеофейки	в) інформація, що була записана, оброблена та розміщена для підтвердження псевдофактів
4. фотофейк	г) інформація, подана, зазвичай від імені очевидців певної події

2. Опануйте ресурс «НотаЄнота», призначений для тих, хто хоче навчитися розпізнавати ворожі впливи, розвивати критичне. Місія кожної гри «Врятувати Єнота з інформаційного полону»

Нейтралізуй ворожі фейки
ТУТ

ВІДСКАНУЙ МЕНЕ

4. Проблемно-пошукове завдання

1. Поміркуйте, які основні правила цифрової гігієни варто дотримуватися в мережі.
2. Визначте, чому важливо формувати культуру кібербезпеки серед учасників освітнього процесу.
3. Проаналізуйте, які ознаки дозволяють ідентифікувати фішингове повідомлення на електронну пошту.
4. Поміркуйте, які інструменти допомагають визначити надійність інтернет джерел та контенту?

КОМПЛЕКС ПРАКТИЧНИХ (ТЕСТОВИХ) ЗАВДАНЬ ДЛЯ САМОКОНТРОЛЮ

1. Що таке кібербезпека?

а) захист інформації від несанкціонованого доступу

б) розробка антивірусних програм

в) написання комп'ютерних вірусів

г) створення паролів

2. Як називається викрадення особистих даних в Інтернеті?

а) кібербулінг

б) фішинг

в) скімінг

г) сталкінг

3. Що таке соціальна інженерія в кібербезпеці?

а) використання соцмереж для кібератак

б) вплив на людину для отримання конфіденційних даних

в) розробка суспільних ініціатив з кібербезпеки

г) дослідження суспільної думки про кіберзагрози

4. Що таке кібергігієна?

а) дотримання правил гігієни під час роботи з комп'ютером

б) комплекс заходів з інформаційної безпеки в інтернеті

в) використання антивірусних програм

г) регулярне очищення комп'ютера від пилу

5. Що таке кібератака?

а) напад з використанням інформаційних технологій з метою заподіяння шкоди

б) розсилка спаму

в) створення комп'ютерного вірусу

г) злам облікового запису в соцмережі

6. Що таке фішинг?

а) інтернет-шахрайство з метою отримання даних користувача

б) поширення комп'ютерних вірусів

в) кіберцькування

г) несанкціонований доступ до пристрою

7. Що таке куки в інтернеті?

а) шкідливе програмне забезпечення

б) мережеві журнали дій користувача

в) невеликі текстові файли з даними для сайтів

г) програми для злому паролів

8. Які дані називають персональними?

а) e-mail, ім'я, адреса, телефон

б) історія пошукових запитів

в) дані банківської карти

г) комп'ютерний логін

9. Що таке кібербулінг?

а) погрози в інтернеті

б) цькування в мережі

в) шахрайство в інтернеті

г) вірусна атака

10. Як називається викрадення облікових даних в інтернеті?

а) фішинг

б) скімінг

в) докінг

г) спуфінг

11. Що таке медіаграмотність у контексті кібербезпеки?

а) розуміння комп'ютерних технологій

б) вміння створювати Zoom-конференції

в) здатність критично оцінювати інтернет-інформацію

г) навички фотошопу

12. Що таке соціальна інженерія?

а) вивчення поведінки в соцмережах

б) розробка суспільних ініціатив з кібербезпеки

в) вплив на людей, щоб виманити конфіденційні дані

г) створення фейкових акаунтів в інтернеті

13. Що таке двофакторна автентифікація?

а) використання сканера відбитків пальців

б) підтвердження особи паролем і кодом

в) біометрична перевірка обличчя

г) аналіз поведінки користувача

14. Ви отримали електронний лист від невідомого Вам відправника із запитанням поділитися своїм паролем для оновлення системи безпеки. Яка дія буде найбезпечнішою?

а) відправити пароль, оскільки лист виглядає офіційно

б) ігнорувати лист і видалити його

в) запитати у колег та друзів, чи отримували вони схожі листи

г) змінити пароль і не реагувати на лист

15. Ви помітили підозрілі активності на своєму банківському акаунті, але отримали SMS-повідомлення з проханням надати свій ПІН-код для підтвердження операцій. Як ви поводитиметесь?

а) надати ПІН-код для підтвердження операцій

б) зателефонувати у банк і повідомити про підозрілі активності

в) ігнорувати SMS-повідомлення та не реагувати

г) звернутися до друзів за порадою

16. Під час користування громадським Wi-Fi Ви помітили, що підключення не зашифроване. Як Ви забезпечите безпеку своїх даних?

а) використовувати громадський Wi-Fi без будь-яких заходів

б) завершити всі сесії та утримуватися від важливих транзакцій

в) змінити паролі для всіх онлайн-акаунтів відразу

г) звернутися до адміністратора мережі для запитання про шифрування

ГЛОСАРІЙ КЛЮЧОВИХ СЛІВ

Антивірусне програмне забезпечення – комп'ютерна програма, яка використовується для запобігання, виявлення та видалення шкідливих програм.

Автентифікація – процес перевірки того, що хтось є саме тією особою, за яку він або вона себе видає, коли намагається отримати доступ до комп'ютера або онлайн-сервісу.

Брандмауер/файрвол – апаратне або програмне забезпечення, призначене для запобігання несанкціонованому доступу до комп'ютера або мережі з іншого комп'ютера або мережі.

Байтінг – залучення жертви до співпраці певним стимулом.

Багатофакторна автентифікація – отримання доказів ідентичності двома та більше незалежними способами, наприклад: знання пароля та відбиток пальця

Вкладення – комп'ютерний файл, надісланий із повідомленням електронної пошти.

Вішинг – специфічна форма фішингу, спроба обдурити когось по телефону з метою видати приватну інформацію, яка буде використовуватися для крадіжки особистих даних.

Вірус-вимагач (ransomware) – тип шкідливого програмного забезпечення, який блокує доступ до ключових компонентів даних/ мережі та вимагає сплати викупу.

Вірус – шкідливе програмне забезпечення, яке завантажується на комп'ютер, а потім запускається, при цьому користувач не знає про це або не знає про усі наслідки такого запуску.

Діпфейк – діпфейк відноситься до будь-якого відео, в якому обличчя дієвої особи були створені або змінені за допомогою штучного інтелекту.

Двофакторна автентифікація – отримання доказів ідентичності двома незалежними способами, наприклад: знання пароля та відбиток пальця

Злам – несанкціоноване вторгнення в комп'ютер або мережу.

Загроза – будь-яке явище, подія або процес, що може завдати шкоди системі або організації.

Інтелектуальна власність – у широкому розумінні термін означає закріплене законом тимчасове виключне право, а також особисті немайнові права авторів на результат інтелектуальної діяльності або засоби індивідуалізації.

Інформаційна війна – це змагання за виплив та контроль над інформаційними ресурсами супротивника.

Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації.

Кукі – невеликі файли, які зберігаються на комп'ютері користувача. Файли cookie дозволяють веб -сайту впізнати вас і відстежувати ваші уподобання.

Крадіжка особистості – злочин, під час якого хтось використовує особисту інформацію, щоб видати себе за когось іншого.

Кібергігієна – методи та кроки, які вживають користувачі комп'ютерів та інших пристроїв для підтримки захищеності систем та підвищення особистої безпеки в мережі Інтернет.

Кібервійна – кібервійна, як правило, відноситься до кібератак, здійснених однією державою проти іншої.

Кібератака – атака через кіберпростір, спрямована на використання русерсів підприємства з метою порушення, вимкнення, знищення або зловмисного контролю обчислювального середовища/інфраструктури, порушення цілісності даних, викрадення інформації.

Логін – ім'я, яке однозначно ідентифікує когось у комп'ютерній системі.

Оновлення – фрагмент програмного коду, який застосовується після встановлення програмного забезпечення, щоб усунути проблему в цьому ПЗ.

Обліковий запис користувача – сукупність даних про користувача, що зберігається комп'ютером для контролю доступу користувача до файлів і програм.

Програмне забезпечення – програми, які використовуються для виконання завдань із комп'ютером.

План реагування на інциденти – план, що передбачає реагування організації на інциденти інформаційної безпеки.

Підвищення поінформованості – навчальна програма, спрямована на підвищення рівня поінформованості про безпеку в організації.

Персональна інформація – дані, що стосуються людини, особу якої можна визначити за їх допомогою.

Пароль – секретна серія символів, що використовуються для автентифікації особи.

Спам – термін, який зазвичай використовується для опису небажаної електронної пошти в Інтернеті.

Соціальна інженерія – мистецтво отримання доступу до будівель, систем або даних на основі використання психології людини, а не через втручання або використання технічних засобів хакерства.

Смішинг – будь-який вид фішингу, що включає передачу текстових повідомленнь.

Скам (шахрайство) – термін, що використовується для опису будь-якого шахрайського бізнесу або схеми, яка забирає гроші чи інші товари у нічого не підозрюваної особи.

Троянський кінь – це тип шкідливого програмного забезпечення, замасковане разом з законним програмним забезпеченням для отримання доступу до систем цільових користувачів.

Фішинг – метод, який використовують злочинці для спроби отримання фінансової чи іншої конфіденційної інформації (як-от: імена користувачів та паролі) від користувачів Інтернету, як правило, шляхом надсилання електронного листа, який виглядає так, начебто його було надіслано справжньоюлегітимною організацією (часто банком). В електронному листі зазвичай міститься посилання на підроблений веб-сайт, який виглядає автентичним.

Хакер – людина, яка володіє знаннями та вміннями аналізувати програмний код чи комп'ютерну систему, змінюючи його функції чи операції та змінюючи його здібності та можливості.

Центр керування безпекою – центр, що відстежує операції в організації для запобігання, виявлення та реагування на будь-які потенційні загрози.

Шпигунські програми – шкідливе програмне забезпечення, яке передає інформацію про діяльність користувача комп'ютера зовнішній третій стороні.

Шкідливе програмне забезпечення – програмне забезпечення, призначене для проникнення в комп'ютери з метою їх інфільтрації та пошкодження або вимкнення комп'ютерів. Англ. malware – скорочена форма від англ. malicious software – «шкідливе програмне забезпечення».

НАЦІОНАЛЬНА АКАДЕМІЯ ПЕДАГОГІЧНИХ НАУК УКРАЇНИ
ДЗВО «УНІВЕРСИТЕТ МЕНЕДЖМЕНТУ ОСВІТИ»
БІЛОЦЕРКІВСЬКИЙ ІНСТИТУТ НЕПЕРЕРВНОЇ ПРОФЕСІЙНОЇ ОСВІТИ
Кафедра технологій навчання, охорони праці та дизайну

КОНСУЛЬТАЦІЙНИЙ ПУНКТ

За консультаціями чи уточненнями окремих питань електронного курсу можна звертатися до викладача Головко Дар'ї Юріївни за

Мобільний телефон: +38 (050) 817 06 72

Електронна пошта: rinadarina88@gmail.com

Соціальні мережі:
https://www.facebook.com/holovkodaria/

ЦИФРОВА БІБЛІОТЕКА

Основні законодавчі та нормативно-правові акти

1. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017 // Офіційний вісник Президента України. – 2017. – № 5. – С. 15. – Ст. 102. URL: https://www.president.gov.ua/documents/472017-21374
2. Закон № 2163-VIII «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради), № 45, с.403, 2017
3. Закон України «Про захист персональних даних» URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
4. Концепція інформаційної безпеки України: Режим доступу: https://www.osce.org/files/f/documents/0/2/175056.pdf
5. Про інформацію : Закон України від 02.10.92 р. № 2657-XII //Відомості Верховної Ради України. – 1992. – № 48. – ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
6. Про кіберзлочинність : Конвенція Ради Європи від 23.11.01 р. № 994-575. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
7. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
8. Стратегія кібербезпеки України (2021 – 2025 роки). Режим доступу: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

Основна література

9. Бараненко Р.В. Кібератаки як одна із форм кібертероризму // Вчені записки Таврійського національного університету ім. В.І. Вернадського, Серія: Технічні науки, Т.32(71), №1,Ч.1, 2021, С.45-50. DOI https://doi.org/10.32838/2663-5941/2021.1- 1/07
10. Богуш В.М., Богуш В.В. Основи кіберпростору, кібербезпеки та кіберзахисту : навч. посіб. Київ : Ліра-К, 2020. 552 с.
11. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко, Л. В. Бурячок, П. М. Складанний, Н. В. Лукова-Чуйко. – Київ: ДУТ – КНУ, 2016. – 178 с.
12. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с
13. Захист дітей у цифровому середовищі: рекомендації для батьків та освітян, 2020. Режим доступу: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/1/za-initsiativi-

mintsifripidgotuvali-rekomendatsii-shchodo-zakhistu-ditey-u-tsifrovomu-seredovishchi/COP-Guidelinesfor-Parents-Educators-UAfin.pdf
14. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. — Харків: Вид. ХНЕУ, 2008. – 352 с.
15. Кібербезпека. аспект 1: соціальні мережі. Міністерств оборони України. [Електронний ресурс]. Режим доступу: http://www.mil.gov.ua/ukbs/shhodenni-kiberzagrozi/kiberbezpeka-aspekt-1-soczialni-merezhi.html
16. Кібервійна : Режим доступу: https://uk.wikipedia.org/wiki/Кібервійна
17. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі : навчальний посібник. – Київ: ВІКНУ, 2016. 286 с.
18. Марущак А. І. Проблеми розслідування кіберзлочинів в Україні // Економіка, фінанси, право. 2018. No 1. С. 23-27.
19. Н.П. Дементієвська, "Формування навичок критичного оцінювання веб-ресурсів і проблема безпеки учнів в інтернеті", Комп'ютер у школі та сім'ї, 7, 46-51, 2015
20. Половенко Л. П., Мерінова С. В. Виявлення ознак соціальної інженерії та технологія протидії соціальним хакерам на підприємстві // Підприємництво та інновації. – 2019. No 10. С. 183-187.
21. Словник термінів з кібербезпеки / За загальною редакцією Копана О.В., Скулиша Є.Д. –К. : ВБ «Аванпост-Прим». – 2012. – 214 с.
22. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. Вступ до кібербезпеки: навч. посіб. – Кропивницький: ЦНТУ, 2022. – 967 с.
23. Т. Савчук, "Соціальна інженерія: як шахраї використовують людську психологію в інтернеті", 30 серпня 2018. [Електронний ресурс]. Режим доступу:https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html
24. Тарасюк А.В. Кібербезпека України на сучасному етапі державоутворення: теоретико правові основи; Одеса: Фенікс, 2020. 404 с.
25. Технологія OSINT: інструменти та методи для захисту інформаційної безпеки: практю посіб. / Т.Ю. Ткачук, І.М. Ничитайло, А.І. Старосєк. Київ: НА СБУ, 2023. 180 с.