НАЦІОНАЛЬНА АКАДЕМІЯ ПЕДАГОГІЧНИХ НАУК УКРАЇНИ
ДЗВО «УНІВЕРСИТЕТ МЕНЕДЖМЕНТУ ОСВІТИ»
БІЛОЦЕРКІВСЬКИЙ ІНСТИТУТ НЕПЕРЕРВНОЇ ПРОФЕСІЙНОЇ ОСВІТИ
КАФЕДРА ТЕХНОЛОГІЇ НАВЧАННЯ, ОХОРОНИ ПРАЦІ ТА ДИЗАЙНУ

КІБЕРБЕЗПЕКА В ЦИФРОВОМУ ОСВІТНЬОМУ СЕРЕДОВИЩІ ЗАКЛАДІВ ПРОФЕСІЙНОЇ ОСВІТИ

електронний навчальний курс

Розробник: Гончарова Ірина Петрівна,

ст. викладач кафедри технологій навчання охорони праці та дизайну

Білоцерківського інституту неперервної професійної освіти

СХВАЛЕНО

кафедрою технологій навчання,
охорони праці та дизайну
протокол № 10 від «12» грудня 2022 р.
Завідувач кафедри _____ О.В.Маслова

Біла Церква – 2022

Затверджено на засіданні кафедри технологій навчання, охорони праці та дизайну.
Протокол № 10 від 12 грудня 2022 року

Схвалено Вченою радою БІНПО ДЗВО «УМО» НАПН України
Протокол № 6 від 21 грудня 2022 року

Рецензенти:

Сороквашин Сергій Володимирович, кандидат педагогічних наук, заступник директора з навчально-методичної роботи Дніпропетровського центру професійно-технічної освіти державної служби зайнятості;

Самойленко Олександр Миколайович, доктор педагогічних наук, доцент, професор кафедри технологій навчання, охорони праці та дизайну Білоцерківського інституту неперервної професійної освіти ДЗВР «УМО» НАПН УКРАЇНИ

Гончарова І.П. Кібербезпека в цифровому освітньому середовищі закладів професійної освіти: електронний навчальний курс / І.П. Гончарова, Біла Церква, БІНПО ДЗВО «УМО» НАПН УКРАЇНИ, 2022. 80 с.

Розвиток інформаційного суспільства передбачає впровадження цифрових інформаційних технологій у всі сфери життя, але це означає і появу нових загроз безпеки. Серед усіх компонентів безпеки з'явився новий і одночасно складний елемент безпеки – кібербезпека. Кібербезпека — це процес застосування заходів безпеки з метою забезпечення конфіденційності, цілісності та доступності даних. Кіберзагрози існують скрізь, де застосовуються інформаційні технології, отже, педагог може у своїй професійній діяльності зіткнутися зі спамом, з вірусами, зі зломом комп'ютера та з багатьма іншими проблемами, на які потрібно не тільки оперативно реагувати, а й вміти запобігати їх появі, а значить постійно згадувати в контексті уроку різні аспекти організації інформаційної безпеки. Педагог повинен мати уявлення про сучасний рівень розвитку інформаційних цифрових технологій.

Актуальність курсу визначається необхідністю сформувати у слухачів курсу додаткової мотивації до вивчення питань інформаційної безпеки. Кібербезпека є найактуальнішою проблемою сучасності. І всі користувачі цифрових технологій роблять усе можливе, аби запобігти витокам конфіденційних даних та зменшити потенційні ризики.

Мета курсу полягає в формуванні у слухачів курсу знань, умінь, навичок та досвіду діяльності, які характеризують етапи формування компетенцій у галузі цифрової економіки та розвитку цифрової грамотності учасників освітнього процесу, освоєнні професійної компетенції у сфері інформаційної безпеки (кібербезпеки).

Електронний курс призначений для педагогічних працівників закладів професійної освіти.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІНФОРМАЦІЯ ДЛЯ ОПРАЦЮВАННЯ

ПИТАННЯ ДЛЯ ОБГОВОРЕННЯ

ТЕМИ ДОПОВІДЕЙ

ПРАКТИЧНЕ ЗАВДАННЯ

ЗВЕРНІТЬ УВАГУ

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

ТЕСТОВИЙ КОНТРОЛЬ ЗНАНЬ

ЗМІСТ ЕЛЕКТРОННОГО НАВЧАЛЬНОГО КУРСУ

АНОТАЦІЯ 5

ПОЯСНЮВАЛЬНА ЗАПИСКА 6

ПРОФІЛЬ ТИПОВОЇ ОСВІТНЬОЇ ПРОГРАМИ

ЕЛЕКТРОННОГО НАВЧАЛЬНОГО КУРСУ 8

ТЕМАТИЧНИЙ ПЛАН ВИКЛАДУ ТА ЗАСВОЄННЯ МАТЕРІАЛУ 11

ЗМІСТ ЕЛЕКТРОННОГО НАВЧАЛЬНОГО КУРСУ ЗА ТЕМАМИ 12

ПЛАН ЛЕКЦІЇ 13

ПЛАНИ СЕМІНАРСЬКИХ ЗАНЯТЬ 30

САМОСТІЙНА РОБОТА 66

КОМПЛЕКС ПРАКТИЧНИХ (ТЕСТОВИХ) ЗАВДАНЬ ДЛЯ САМОКОНТРОЛЮ....68

ГЛОСАРІЙ КЛЮЧОВИХ СЛІВ 76

ЦИФРОВА БІБЛІОТЕКА 81

АНОТАЦІЯ

Кіберзагрози існують скрізь, де застосовуються інформаційні технології, отже, педагог може у своїй професійній діяльності зіткнутися зі спамом, з вірусами, зі зломом комп'ютера та з багатьма іншими проблемами, на які потрібно не тільки оперативно реагувати, а й вміти запобігати їх появі, а значить постійно згадувати в контексті уроку різні аспекти організації інформаційної безпеки. В сучасних закладах освіти комп'ютерні технології використовуються майже при вивченні всіх навчальних предметів. Саме тому, необхідно вдосконалювати сучасну професійну підготовку педагогів у сфері інформаційних технологій, а отже, і у сфері кібербезпеки. Отже, педагог повинен мати уявлення про сучасний рівень розвитку інформаційних цифрових технологій.

Актуальність курсу визначається необхідністю сформувати у слухачів курсу додаткової мотивації до вивчення питань інформаційної безпеки. Кібербезпека є найактуальнішою проблемою сучасності. І всі користувачі цифрових технологій роблять усе можливе, аби запобігти витокам конфіденційних даних та зменшити потенційні ризики.

Мета курсу полягає в формуванні у слухачів курсу знань, умінь, навичок та досвіду діяльності, які характеризують етапи формування компетенцій у галузі цифрової економіки та розвитку цифрової грамотності учасників освітнього процесу, освоєнні професійної компетенції у сфері інформаційної безпеки (кібербезпеки).

Електронний курс призначений для педагогічних працівників закладів професійної (професійно-технічної) освіти.

Бюджет навчального часу становить 8 годин, з яких: лекція (2 год.), семінарське заняття (4 год.), самостійна робота (2 год.)

Зміст курсу

ТИПОВА ОСВІТНЯ ПРОГРАМА ЕЛЕКТРОННОГО КУРСУ

1. Пояснювальна записка

Розвиток інформаційного суспільства передбачає впровадження цифрових інформаційних технологій у всі сфери життя, але це означає і появу нових загроз безпеки. Серед усіх компонентів безпеки з'явився новий і одночасно складний елемент безпеки – кібербезпека.

Кібербезпека – це сукупність технічних та соціальних засобів, стратегій, принципів для забезпечення захисту суспільства від загроз та впливів з небажаними наслідками, що походять від інтернет-середовища. Кібербезпека — це процес застосування заходів безпеки з метою забезпечення конфіденційності, цілісності та доступності даних. Кібербезпека покликана захистити дані на етапі їх обміну та збереження. В законі України «Про основні засади здійснення кібербезпеки України» кіберпростір визначається як «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних», а кібербезпека, як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі». У зв'язку з цим велике значення набуває проблема культури безпечної поведінки у кіберпросторі.

Закон України «Про основні засади здійснення кібербезпеки України» зазначає, що розвиток безпечного, стабільного і надійного кіберпростору має полягати в тому числі і завдяки «підвищенню цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту».

В сучасних закладах освіти комп'ютерні технології використовуються майже при вивченні всіх навчальних предметів. Саме тому, необхідно вдосконалювати сучасну професійну підготовку педагогів у сфері інформаційних технологій, а отже, і у сфері кібербезпеки.

Зміст курсу

Кіберзагрози існують скрізь, де застосовуються інформаційні технології, отже, педагог може у своїй професійній діяльності зіткнутися зі спамом, з вірусами, зі зломом комп'ютера та з багатьма іншими проблемами, на які потрібно не тільки оперативно реагувати, а й вміти запобігати їх появі, а значить постійно згадувати в контексті уроку різні аспекти організації інформаційної безпеки. Педагог повинен мати уявлення про сучасний рівень розвитку інформаційних цифрових технологій.

Актуальність курсу визначається в необхідності сформувати у слухачів курсу додаткової мотивації до вивчення питань інформаційної безпеки. Кібербезпека є найактуальнішою проблемою сучасності. І всі користувачі цифрових технлогій роблять усе можливе, аби запобігти витокам конфіденційних даних та зменшити потенційні ризики.

Програма знайомить слухачів

– з основами кібербезпеки;

– з практикою застосування знань з основ кібербезпеки у цифровому освітньому середовищі;

– практикою застосування окремих елементів захисту інформації при побудові освітнього процесу.

Завдання курсу:

– дати знання в області інформаційної кібербезпеки;

– сформувати розуміння технологій інформаційної безпеки та вміння застосовувати правила кібербезпеки;

– підвищення цифрової грамотності.

Мета курсу: сформувати та розвинути у слухачів курсу професійні компетенції, що дозволяють їм застосовувати сучасні технології захисту інформації, вибирати засоби та інструменти захисту інформації, які мінімізують загрози несанкціонованого доступу до даних.

Досягнення зазначеної мети передбачає розв'язання сполуки завдань:

– поглиблення знань в області інформаційної кібербезпеки;

– розширення уявлення про практику застосування знань з основ кібербезпеки в цифровому освітньому середовищі;

– розширення уявлення про практику застосування окремих елементів захисту інформації при побудові освітнього процесу.

– розвиток інформаційно-цифрової компетентності педагогічних працівників закладів професійної (професійно-технічної) освіти;

– набуття практичного досвіду застосування заходів для забезпечення захисту інформаційних систем.

Зміст курсу

Електронний курс призначений для педагогічних працівників закладів професійної (професійно-технічної) освіти.

Бюджет навчального часу становить 8 годин (0,26 кредиту ЄКТС).

Освітній процес здійснюється за такими **формами:** *лекція (2 год.), семінарське заняття (4 год.), самостійна робота (2 год.)*

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

2. Профіль Типової освітньої програми електронного навчального курсу

Профіль Типової освітньої програми електронного навчального курсу «*Кібербезпека в цифровому освітньому середовищі закладів професійної освіти*»		
Обсяг курсу		**На опанування матеріалів електронного навчального курсу передбачено 8 академічних годин**, що відповідають **0,26 ЄКТС-кредиту**
Рівень програми		Безперервний професійний розвиток фахівців шляхом формальної, неформальної та інформальної освіти
А	**Мета**	
	Формуванні у слухачів курсу знань, умінь, навичок та досвіду діяльності, які характеризують етапи формування компетенцій у галузі цифрової економіки та розвитку цифрової грамотності учасників освітнього процесу, освоєнні професійної компетенції у сфері інформаційної безпеки (кібербезпеки).	
В	**Характеристика Типової програми**	
1	Функціональна спрямованість	Розвиток професійних компетенцій слухачів курсів підвищення кваліфікації та забезпечення безпеки персональних даних в закладі професійної освіти
2	Фокус Типової програми	Акцент на: – поглиблення знань в області інформаційної кібербезпеки; – розширення уявлення про практику застосування знань з основ кібербезпеки в цифровому освітньому середовищі; – розширення уявлення про практику застосування окремих елементів захисту інформації при побудові освітнього процесу. – розвиток інформаційно-цифрової компетентності педагогічних працівників закладів професійної (професійно-технічної) освіти; – набуття практичного досвіду застосування заходів для забезпечення захисту інформаційних систем.
3	Орієнтація Типової програми	Типова освітня програма орієнтована на безперервний професійний розвиток педагогічних працівників та розвиток їх професійних компетентностей в області інформаційної кібербезпеки
4	Особливості Типової програми	Типова програма орієнтована спрямована на розвиток цифрових компетентностей сучасного педагога

Зміст курсу

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
D	**Стиль і методика навчання**	
	Підходи до викладання і навчання	Навчання відбувається за очною, дистанційною, очно-дистанційною формами з використанням компетентнісного, діяльнісного, інформаційного, комунікаційного, андрагогічного, особистісно зорієнтованого підходів
	Система оцінювання	Зараховано / не зараховано
E	**Ключові компетентності**	
	Інтегральна компетентністт	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
	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.
	Фахові компетентності	***предметно-методична*** **-** використання у професійній діяльності системи наукових і методичних знань, умінь з кібербезпеки, 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; інформаційна й медіа-грамотність, алгоритмічне мислення, навички безпеки в Інтернеті та кібербезпеці; розуміння етики роботи з інформацією; ***інноваційна*** – система мотивів, знань, умінь, навичок, особистісних якостей педагога, що забезпечує ефективність використання нових педагогічних технологій у роботі зі здобувачами освіти; ***навчання впродовж життя*** – здатність до пошуку та засвоєння нових знань, набуття нових вмінь і навичок, організації навчального процесу (власного і колективного), зокрема через ефективне керування ресурсами та інформаційними потоками, вміння визначати навчальні цілі та способи їх досягнення, вибудовувати свою освітньо-професійну траєкторію, оцінювати власні результати навчання, навчатися впродовж життя

Зміст курсу

		психологічна - усвідомлення ціннісної значущості фізичного, психічного і морального здоров'я суб'єктів освітнього процесу, здатність сприяти їхньому творчому становленню та індивідуалізації ; ***педагогічне партнерство*** – вміння організувати навчання на засадах дитиноцентризму та індивідуального підходу до кожного здобувача освіти. Ґрунтується на цінностях довіри, взаємоповаги та підтримки, доброзичливості; ***проєктувальна*** – заснована на знаннях, уміннях, особистісному досвіді і ціннісних орієнтаціях педагога, які сприяють ефективній підготовці та впровадженню освітніх проектів; ***андрагогічна компетентність*** – уміння визначати освітні потреби і запити, ураховувати особливості мотивації, процесу навчання, визначати результати навчання, спонукати до рефлексії ***прогностична*** – вміння педагога визначити напрямок своєї діяльності, її конкретні цілі і завдання на кожному етапі виховної роботи, і передбачати кінцевий результат; ***управлінська*** –вміння планувати, організовувати контролювати професійну діяльність відповідно до сучасних вимог; володіти технологіями науково-методичного супроводу освітнього процесу в умовах реформ і соціальних трансформацій; ***оцінювально-аналітична*** – здатність до здійснення оцінювання результатів навчання здобувачів освіти, аналізу їх результатів навчання; здатність до забезпечення самооцінювання та взаємооцінювання результатів навчання здобувачів освіти; ***соціально-громадянська –*** усі форми поведінки, які потрібні для ефективної та конструктивної участі у громадському житті, в сім'ї, на роботі. Уміння працювати з іншими на результат, попереджати і розв'язувати конфлікти, досягати компромісів. Повага до закону, дотримання прав людини і підтримка соціокультурного різноманіття; ***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. Вміння раціонально вести себе як споживач, ефективно використовувати індивідуальні заощадження, приймати доцільні рішення
F	**Програмні результати навчання**	
	Знання і розуміння	– вміння використовувати засоби інформаційних та комунікаційних технологій у вирішенні когнітивних, комунікативних та організаційних завдань з дотриманням вимог ергономіки, техніки безпеки, гігієни,

Зміст курсу

		ресурсозбереження, правових та етичних норм, норм інформаційної безпеки; – знання принципів безпечної роботи з мобільними пристроями, зокрема, смартфонами та планшетами; – розуміння основ правових аспектів використання комп'ютерних програм та роботи в Інтернеті; – вміння використовувати сучасні технології захисту інформації, вибирати засоби та інструменти захисту інформації, що мінімізують загрози несанкціонованого доступу до даних.
	Розвинені вміння	– стійкі навички керування інформаційними системами в нестандартних ситуація; – аналіз змісту навчального матеріалу з метою раціонального, логічного і доступного його відбору, структурування по навчальним одиницям; – створення комплексного методичного забезпечення предметів за професійною спрямованістю
	Диспозиції (цінності, ставлення)	– необхідність, доцільність та можливість застосування основ кібербезпеки у професійній підготовці кваліфікованих робітників; – важливість підвищення якості освітнього процесу у ЗП(ПТ)О шляхом формування на якісно новому рівні культури розумової праці та взаємодії з оточуючими, відповідального ставлення до питань цифрової безпеки
Ключові слова Кібербезпека, Кіберінцидент, кібератака, кіберзагроза, кіберзахист, кіберзлочин (комп'ютерний злочин), кіберзлочинність - сукупність кіберзлочинів, кіберпростір, кібертероризм, кібершпигунство, національні електронні інформаційні ресурси, системи електронних комунікацій		

3. ТЕМАТИЧНИЙ ПЛАН ВИКЛАДУ ТА ЗАСВОЄННЯ МАТЕРІАЛУ

№ з/п	Тематичний план	Формальні заняття, кількість годин			
		Лекції	Семінарське заняття	Самостійна робота	Разом
1	Поняття кібербезпеки. Онлайн та офлайн ідентифікація. Методи та засоби захисту конфіденційної інформації, персональних даних учасників освітнього процесу	2	2		4
2	Забезпечення інформаційної безпеки учасників освітнього процесу в ЗП(ПТ)О		2		2
3	Удосконалення рівня цифрової компетентності учасників освітнього процесу з кібербезпеки: інструменти, технології			2	2
	Разом	**2**	**4**	**2**	**8**

ЗМІСТ ЕЛЕКТРОННОГО НАВЧАЛЬНОГО КУРСУ ЗА ТЕМАМИ

Тема 1. Поняття кібербезпеки. Он-лайн та оф-лайн ідентифікація. Методи та засоби захисту конфіденційної інформації, персональних даних учасників освітнього процесу

Поняття кібербезпеки. Конфіденційність, цілісність та доступність даних. Наслідки порушення безпеки. Он-лайн та оф-лайн ідентифікація. Приватні дані та місця їх розташування. Причини викрадення даних. Бездротові з'єднання, автентифікація та стійкі паролі. Методи та засоби захисту конфіденційної інформації при використанні Інтернету.

Типи порушників у сфері кібербезпеки. Внутрішні та зовнішні загрози. Правові проблеми кібербезпеки. Захист організації.

Тема 2. Забезпечення інформаційної безпеки учасників освітнього процесу в ЗП(ПТ)О

Інформаційна безпека здобувачів освіти. Документи, що регламентують роботу закладу освіти з персональними даними, плани заходів щодо забезпечення інформаційної безпеки здобувачів освіти. Кібербезпека учасників освітнього процесу.

Тема 3. Удосконалення рівня цифрової компетентності учасників освітнього процесу з кібербезпеки: інструменти, технології

Сучасні міжнародні програми у галузі кібербезпеки, напрями подальшого підвищення кваліфікації. Знайомство із середовищем дистанційної освіти Cisco NetAcad міжнародної мережевої академії Cisco.

ПЛАН ЛЕКЦІЙ

Тема 1. Поняття кібербезпеки. Он-лайн та оф-лайн ідентифікація. Методи та засоби захисту конфіденційної інформації, персональних даних учасників освітнього процесу (2 год)

1. Поняття кібербезпеки, кібератаки. Конфіденційність, цілісність та доступність даних.
2. Типи загроз. Способи захисту інформації від загроз.
3. Онлайн (online) та офлайн (offline)-ідентифікація. Захист особистих даних.
4. Захист організації.

1. Поняття кібербезпеки, кібератаки. Конфіденційність, цілісність та доступність даних

Кібербезпека є найважливішим питанням сьогодення, оскільки в сучасному цифровому світі кіберзагрози та атаки становляться все частіше. Кожного дня ми чуємо, що зламали чиюсь сторінку у соціальній мережі і розсилаються з нею повідомлення, що у когось з картки пропали гроші, що хтось розсилає повідомлення з вашої електронної пошти. Зловмисники тепер використовують складніші методи для націлювання на системи. Піддаються їхньому впливу усі: люди, малий бізнес або організації і установи. Таким чином, усі ці організації, чи то IT, чи не IT-компанії, усвідомили важливість кібербезпеки і зосередилися на вжитті всіх можливих заходів для боротьби з кіберзагрозами. Оскільки нам подобається все підключати до Інтернету, це також збільшує ймовірність вразливостей, порушень та недоліків. Минули часи, коли паролів було достатньо для захисту системи та її даних. Ми всі хочемо захистити наші особисті та професійні дані, тому Cyber Security – це те, що ми повинні знати для забезпечення захисту даних.

Під'єднання до електронної інформаційної мережі стало невід'ємною частиною нашого повсякденного життя. Усі організацій, установи, в тому числі і освітні, використовують цю мережу для ефективного функціонування. Електронна інформаційна мережа використовується для збору, обробки, зберігання та обміну великою кількістю цифрової інформації. Чим більше цифрової інформації збирається і чим частіше вона спільно використовується, тим важливішим стає захист цієї інформації забезпечення національної безпеки та економічної стабільності.

Кібербезпека – це сукупність технічних і соціальних засобів, стратегій, принципів для забезпечення захисту суспільства від загроз і впливів з небажаними наслідками, що походять від інтернет-середовища.

Кібербезпека в цілому – це дуже широкий термін, але він ґрунтується на трьох фундаментальних поняттях, відомих як «CIA»: конфедеційність, цілісність, доступність. Ця модель призначена для керівництва організацією політиками кібербезпеки у сфері інформаційної безпеки (InfoSec).

Конфіденційність, цілісність і доступність – це запорука ефективного захисту даних та безпеки інфраструктури організації. Ці три поняття – основоположні принципи для впровадження плану InfoSec.

Якщо коротко, інформаційна безпека — це гарантія того, що співробітники організації зможуть переглядати та редагувати потрібні їм дані, при цьому не дозволяючи нікому більше отримати доступ до них.

При розгляді безпеки інформаційних систем звичайно виділяють дві групи проблем: *безпека комп'ютера і мережева безпека*.

До *безпеки комп'ютера* відносять всі проблеми захисту даних, що зберігаються і обробляються комп'ютером, який розглядається як автономна система. Ці проблеми вирішуються засобами операційних систем та програм, таких як бази даних, а також вбудованими апаратними засобами комп'ютера.

Під *мережевою безпекою* розуміють всі питання, пов'язані з взаємодією пристроїв в мережі, це перш за все захист даних у момент їх передачі по лініях зв'язку та захист від несанкціонованого віддаленого доступу в мережу. І хоча часом проблеми комп'ютерної і мережної безпеки важко відокремити один від одного, настільки тісно вони пов'язані, цілком очевидно, що мережева безпека має свою специфіку.

Автономно працюючий комп'ютер можна ефективно захистити від зовнішніх замахів різноманітними способами, наприклад, просто замкнути на замок клавіатуру або

зняти жорсткий накопичувач і помістити його в сейф. Комп'ютер, що працює в мережі, за визначенням не може повністю відгородитися від світу, він повинен спілкуватися з іншими комп'ютерами, можливо, навіть віддаленими від нього на велику відстань, тому забезпечення безпеки в мережі є завданням значно складнішою. Логічний вхід чужого користувача у ваш комп'ютер є штатною ситуацією, якщо ви працюєте в мережі. Забезпечення безпеки в такій ситуації зводиться до того, щоб зробити це проникнення контрольованим – кожному користувачеві мережі повинні бути чітко визначені його права щодо доступу до інформації, зовнішніх пристроїв та виконання системних дій на кожному з комп'ютерів мережі.

Крім проблем, що породжуються можливістю віддаленого входу в мережеві комп'ютери, мережі за своєю природою схильні до ще одного виду небезпеки – перехоплення та аналізу повідомлень, переданих по мережі, а також створення «помилкового» трафіку. Більша частина коштів забезпечення мережної безпеки спрямована на запобігання саме цього типу порушень.

Питання мережевої безпеки набувають особливого значення зараз, коли при побудові корпоративних мереж спостерігається перехід від використання виділених каналів до публічних мереж (Інтернет, frame relay). Постачальники послуг публічних мереж поки рідко забезпечують захист даних користувача при їх транспортуванні по своїх магістралях, покладаючи на користувачів турботи по їх конфіденційності, цілісності та доступності.

Безпечна інформаційна система – це система, яка, по-перше, захищає дані від несанкціонованого доступу, по-друге, завжди готова надати їх своїм користувачам, а по-третє, надійно зберігає інформацію і гарантує незмінність даних. Таким чином, *безпечна система* за визначенням має *властивості конфіденційності, доступності та цілісності*.

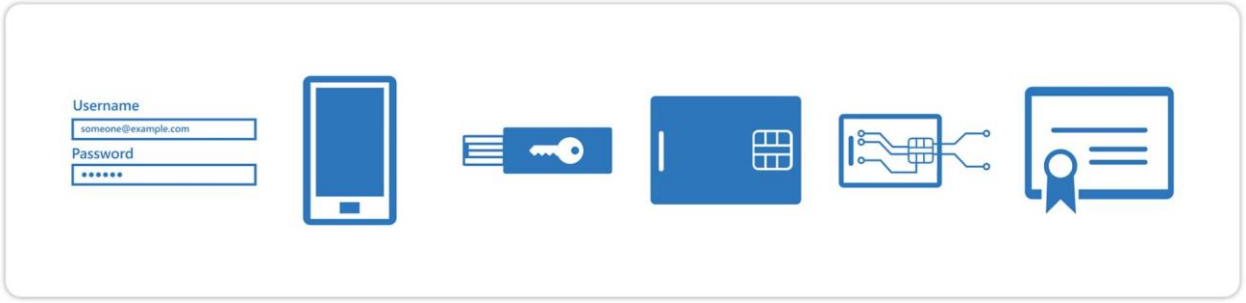
1) ***Конфіденційність (confidentiality)*** – гарантія того, що секретні дані будуть доступні тільки тим користувачам, яким цей доступ дозволений (такі користувачі називаються авторизованими).

Конфіденційність – це основний компонент InfoSec, який полягає в тому, що доступ до інформації можуть отримувати лише авторизовані користувачі. Шифрування даних, багатофакторна автентифікація та захист від втрати даних – це приклади інструментів, які підприємства можуть використовувати для забезпечення конфіденційності інформації.

Що таке багатофакторна автентифікація (БФА)?

Багатофакторна автентифікація (БФА) додає ще один рівень захисту під час входу. Під час доступу до облікових записів або програм користувачі проходять додаткову перевірку ідентичності, наприклад сканують відбиток пальця чи вводять код із телефона.

Багатофакторна автентифікація (БФА) за допомогою хмарної служби *Azure Active Directory (Azure AD)* допомагає захистити доступ до даних і програм, не ускладнюючи роботу для користувачів. Azure AD використовують для проходження багатофакторної автентифікації при доступі до ресурсів організації, наприклад таких як Microsoft 365. Додатковий етап перевірки посилює безпеку під час автентифікації, а сама перевірка відбувається простими й одночасно надійними методами.



2) ***Доступність (availability)*** – гарантія того, що авторизовані користувачі завжди будуть отримувати доступ до даних. Доступність говорить про те, що дані відкриті лише для тих, у кого є відповідні дозволи.

3) ***Цілісність (integrity)*** – гарантія збереження даними правильних значень, яка забезпечується забороною для неавторизованих користувачів будь-яким чином змінювати, модифікувати, руйнувати або створювати дані.

Будь яка організація має підтримувати цілісність даних протягом усього їхнього життєвого циклу. Організації з розвинутим компонентом InfoSec визнають важливість використання точних і надійних даних та не дозволять неавторизованим користувачам отримувати доступ до них, змінювати їх або керувати ними. Такі інструменти, як дозволи для файлів, керування ідентичностями й елементи керування доступом користувачів, забезпечують цілісність даних.

Вимоги безпеки можуть змінюватися залежно від призначення системи, характеру використовуваних даних і типу можливих загроз. Важко уявити систему, для якої були б не важливі властивості цілісності та доступності, але властивість конфіденційності не завжди є обов’язковим.

Наприклад, якщо ви публікуєте інформацію в Інтернеті на Web-сервері і вашою метою є зробити її доступною для найширшого кола людей, то конфіденційність в даному випадку не потрібно. Проте вимоги цілісності та доступності залишаються актуальними.

Поняття конфіденційності, доступності та цілісності можуть бути визначені не тільки по відношенню до інформації, але і до інших ресурсів обчислювальної мережі, наприклад зовнішніх пристроїв або додатків. Існує безліч системних ресурсів, можливість

«незаконного» використання яких може призвести до порушення безпеки системи.

Наприклад, необмежений доступ до пристрою друку дозволяє зловмисникові отримувати копії, роздруковувати документи, змінювати параметри налаштування, що може призвести до зміни черговості робіт і навіть до виведення пристрою з ладу. Властивість конфіденційності, застосована до пристрою друку, можна інтерпретувати так, що доступ до пристрою мають ті і тільки ті користувачі, яким цей доступ дозволений, причому вони можуть виконувати тільки ті операції з пристроєм, що для них визначено. Властивість доступності до пристрою означає його готовність до використання кожного разу, коли в цьому виникає необхідність. А властивість цілісності може бути визначена як властивість незмінності параметрів налаштування цього пристрою. Легальність використання мережевих пристроїв важлива, оскільки вона впливає на безпеку даних. Пристрої можуть надавати різні послуги: роздрук текстів, відправлення факсів, доступ до Інтернету тощо. Незаконне використання мережевих пристроїв завдає матеріальної шкоди організації (підприємству, установі), а також є порушенням безпеки системи.

2. Типи загроз. Способи захисту інформації від загроз.

Кібербезпека – це безпека IT систем (обладнання і програм). Наскільки ваш комп’ютер або веб-сайт захищений від хакерської атаки – це саме і є питання кібербезпеки.

Кібератака – це спроба реалізації загрози. Тобто, це дії кіберзловмисників або шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу.

Кібератаки – це загальна термінологія, яка охоплює велику кількість тем:

- Порушення цілості систем і даних, що зберігаються всередині
- Несанкціонований доступ до конфіденційної інформації
- Порушення нормального функціонування організації
- Використання атак для шифрування даних і вилучення грошей у жертви

Атаки становляться все більш інноваційними, що може порушити безпеку та взломати систему. Тому дуже складно подолати цю проблему та дати відсіч цим атакам.

Більшість сучасних кібератак вважаються змішаними атаками. Змішані атаки використовують одразу кілька методів, щоб проникнути до системи і здійснити атаку. Коли атаці неможливо запобігти, завдання експерта з кібербезпеки полягає у зменшенні наслідків нападу.

Щоб зрозуміти необхідність заходів кібербезпеки, коротко розглянемо типи загроз та атак.

1. Віруси вимагачі (Ransomware - англ. ransom — викуп і software — програмне забезпечення). Це шкідливе програмне забезпечення, яке блокує пристрій або шифрує його вміст, вимагаючи гроші у жертв. За певну плату оператори шкідливого коду обіцяють відновити доступ до інфікованої машини або даних**.**

Серед сумнозвісних шифрувальників, які шкодили користувачам Windows – WannaCry, Bad Rabbit і Petya.

У більшості випадків програма-вимагач відображає на екрані повідомлення, що ваш комп'ютер заблокований, або додає текстовий файл (повідомлення) до відповідних папок. Багато сімейств програм-вимагачів також змінюють розширення зашифрованих файлів.

Як працює програма-вимагач? Оператори програм-вимагачів використовують багато різних технік інфікування:

- **Шифрування диску** та блокування доступу користувача до операційної системи.
- **Блокування екрану** користувача.
- **Шифрування даних** на диску жертви.
- Блокування пристроїв Android шляхом **зміни коду доступу** для заблокування пристрою користувача.

Загроза захована усередині іншого файлу або програми, яка виглядає настільки безвинно, що користувач спокійно їх відкриває: вкладення в електронні листи, відео зі

сторінок сумнівного походження або навіть системні оновлення від особи надійних програм, таких як Windows або Adobe Flash. Після завантаження на комп'ютер шкідлива програма активується і блокує всю операційну систему, після чого запустить попередження із загрозою і з зазначенням суми викупу, яку треба заплатити за «порятунок» всієї інформації. Ці повідомлення розрізняються залежно від типу шкідливої програми з якою Ви зіткнулися: піратський контент, порнографія, помилковий вірус. Щоб додатково налякати жертву, іноді додається IP-адрес, назви Вашого Інтернет-провайдера або навіть фотографія, перехоплена з Вашої вебкамери. При цьому комп'ютер залишається працездатним, але всі файли користувача виявляються недоступними. Інструкцію та пароль для розшифрування файлів зловмисник обіцяє прислати за гроші.

Однак немає ніякої гарантії, що кіберзлочинці виконають свою обіцянку (а іноді вони не можуть це зробити навмисно або через некомпетентне кодування).

Є декілька способів, які допоможуть захистити комп'ютер від здирників та інших шкідливих програм:

– Регулярне оновлення компонентів операційної системи.

– Тримати програмне забезпечення на комп'ютері в актуальному стані оновлюючи його.

– Тримати увімкненим мережевий екран.

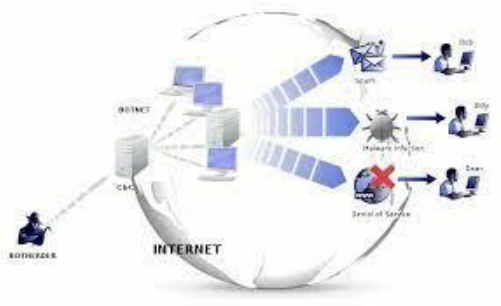
– Не відкривати спам-повідомлення електронної пошти та не відвідувати підозрілі вебсайти.

– Використовувати відомі антивіруси для захисту від шкідливих програм та оновлювати антивірусні бази.

– Перед першим запуском нових програм перевіряти їх антивірусом.

– Періодично виконувати резервне копіювання важливих даних.

2. Атаки ботнетов. Ботнет — це мережа комп'ютерів, інфікована шкідливим програмним забезпеченням. Кіберзлочинці використовують ботнет-мережі, які складаються з великої кількості комп'ютерів для різних зловмисних дій без відома користувачів.



Деякі з атак ботнетів включають:

– Розподілені атаки типу «відмова в обслуговуванні» (DDoS – Distributed Denial of Service).

– Розповсюдження спам-листів.

– Крадіжка конфіденційних даних.

– Встановлення шпигунських програм.

Комп'ютер може потрапити в мережу ботнету через встановлення певного програмного забезпечення, без відома користувача. Трапляється це зазвичай через:

– Інфікування комп'ютера вірусом через вразливість в ПЗ (помилки в браузерах, поштових клієнтах, програмах перегляду документів, зображень, відео).

– Недосвідченість або неуважність користувача — шкідливе ПЗ маскується під «корисне програмне забезпечення».

– Використання санкціонованого доступу до комп'ютера (рідко).

– Підбір адміністративного пароля до мережевих ресурсів зі спільним доступом (наприклад, до $ADMIN, що дозволяє віддалено виконати програму) — переважно в локальних мережах.

Якщо комп’ютер став частиною ботнет-мережі, то це може негативно впливати на роботу комп’ютера. Обчислювальна потужність одного ботнету дозволяє здійснювати декілька зловмисних дій швидко та часто без виявлення. Наприклад, у 2016 році ботнет був використаний для створення найбільшої DDoS-атаки в історії, яка спричинила збої у роботі таких сайтів як Twitter, Amazon та Netflix.

Щоб не стати частиною ботнету, важливо дотримуватися таких правил безпеки:

– Виконувати регулярне оновлення програмного забезпечення та виправлення помилок.

– Використовувати рішення для забезпечення безпеки в Інтернеті, до яких входить захист від ботнет-атак. Такі рішення виявляють та блокують загрози та використовують брандмауер (Брандмауер (Brandmauer) – це комп'ютерна програма, метою якої є захист комп'ютера від вірусів і хакерських атак) для фільтрації зв'язку між комп'ютером та Інтернетом.

– Необхідно бути обережним, завантажуючи файли або програми та відкриваючи вкладення.

3. Атаки соціальної інженерії. Низка не технічних прийомів маніпулювання користувачами, які використовуються кіберзлочинцями під час атак.

Соціальна інженерія – поширена тактика, яку використовують кіберзлочинці для збору конфіденційної інформації користувача. Вся інформація, яку вводить користувач, клонується та використовується для фінансових шахрайств, шахрайства з ідентифікацією тощо. Варто сказати про вірус ZEUS, який активний з 2007 року та використовується як метод соціальної атаки для крадіжки банківських даних жертв. Поряд із фінансовими втратами атаки соціальної інженерії здатні завантажувати інші руйнівні загрози для відповідної системи.

Більшість методів соціальної інженерії не вимагають особливих технічних знань з боку зловмисників, а отже використовувати ці методи може будь-хто — від дрібних злодіїв до досвідчених кіберзлочинців.

Існує багато методик, які підпадають під загальний термін соціальної інженерії в галузі кібербезпеки. Серед найвідоміших методик — спам та фішинг.

Спам — це масове розсилання небажаних листів. Найчастіше спам — це лист електронної пошти, який надсилається одразу на велику кількість адрес, але він також може бути доставлений через миттєві повідомлення, SMS та соціальні мережі. Власне, спам не є соціальною інженерією, однак в деяких кампаніях використовуються його види, такі як фішинг, цілеспрямований фішинг (spearphishing), вішинг (vishing), смішинг (smishing), а також поширення шкідливих вкладень або посилань.

Фішинг (саме слово є омофоном англійського слова «Fishing» (рибалка), оскільки техніка використовує ту ж логіку «вилову») — це форма кібератаки, під час якої злочинець намагається завойовувати довіру жертви для виманювання конфіденційної інформації. Для отримання даних зловмисники також створюють відчуття терміновості або застосовують тактику залякування. Варто зазначити, що фішингові кампанії можуть бути націлені на велику кількість випадкових користувачів або конкретну особу чи групу.

Цілеспрямований фішинг — це форма фішингу, під час якої зловмисник надсилає повідомлення, спрямовані на конкретну групу людей, або навіть просто окрему особу з метою викрадення даних або маніпулювання ними в зловмисних цілях.

Вішинг та смішинг — це методи соціальної інженерії, подібні до фішингу, але здійснюються не через електронну пошту. Зокрема, вішинг реалізовується через шахрайські телефонні дзвінки, а для смішингу використовуються текстові SMS-повідомлення, які містять шкідливі посилання або вміст.

Яскравий приклад — дзвінок нібито з банку. Зловмисники, вдаючи із себе співробітників банку, вигадують різні приводи для виманювання даних. Наприклад, кажуть, що відбулося блокування карти, і служба безпеки банку проводить звіряння особистих даних клієнтів для убезпечення їх від шахрайства. Іншим прикладом є схеми типу «Ваш родич потрапив в аварію чи поліцію». Найчастіше зловмисники здійснюють такого роду дзвінки вночі або рано вранці, коли людина сонна, погано міркує. Шахраї здебільшого розмовляють чітко, впевнено та помірно швидко, щоб не дати змоги жертві зважити ситуацію та поміркувати. При дзвінках «із поліції» шахраї роблять ставку на розгубленість жертви та застосовують методи психологічного тиску, змушуючи особу «вирішувати справу зараз і вже, оскільки немає часу зволікати».

SMS-фішинг (смішинг) — різновид фішингу, який здійснюється через SMS-розсилки. Одним із яскравих прикладів є SMS-повідомлення нібито про виграш великої суми грошей або автомобіля. Однак, щоб отримати виграш, потрібно внести 10% за «оформлення» необхідної документації тощо. Також SMS-шахрайством є повідомлення від «банків».

«Дорожнє яблуко» («road apple»), або «Троянський кінь», — це метод атаки, який передбачає підкинути співробітнику компанії чи установи фізичний носій інформації (флеш-накопичувач, диск) зі шкідливим програмним забезпеченням. Носій може мати логотип компанії чи надпис, що зацікавить співробітника, наприклад, «Список на звільнення», «Заробітна плата. Жовтень» тощо. Щойно співробітник вставить такий носій у комп'ютер, він запустить шкідливий код, який надасть хакеру віддалений доступ до мережі.

Шкідливе програмне забезпечення, ціль якого викликати у жертви почуття страху чи тривоги та таким чином змусити її встановити небезпечний код на пристрій. Поширеними є випадки, коли користувачам відображалось повідомлення про нібито інфікування пристрою загрозою, для видалення якої необхідно завантажити антивірус (який, насправді, є шкідливим програмним забезпеченням).

«Зворотна соціальна інженерія» — це вид соціальної інженерії, за якої особа сама звертається до шахрая та повідомляє свої конфіденційні дані. Одним із можливих сценаріїв є, коли шахрай надсилає співробітникам компанії нібито нові номери телефонів служби технічної підтримки. Цілком імовірно, що через певний час хтось із співробітників зателефонує і шахрай зможе вивідати інформацію, яка його цікавить.

Складна атака через проміжну ціль («Supply chain attack») — це кількаступенева атака, в ході якої хакер атакує не напряму організацію, яка його цікавить, а менш захищену проміжну організацію чи установу, а вже через неї компрометує ту ціль, яка від самого початку його цікавила.

Наприклад, хакер обрав своєю ціллю банк, однак після його вивчення зрозумів, що установа має високий рівень захисту і просто так її не скомпрометувати. У такому разі хакер може сфокусуватися на атаці підрядників, наприклад, на невеликій компанії, яка розробляє або обслуговує сайт чи бази даних банку. Невеликі компанії зазвичай менш захищені, а тому скомпрометувати їх набагато простіше.

Як здійснюються атаки з використанням соціальної інженерії?

Існує декілька ознак, які допоможуть ідентифікувати таку атаку. Зокрема, одна з них — погана граматика та правопис. Ще однією

помітною ознакою є почуття терміновості, яке зловмисники намагаються створити для зменшення пильності жертви. Будь-який запит щодо конфіденційних даних також має викликати підозру: авторитетні компанії ніколи не просять відправити їм паролі або інші особисті дані електронною поштою або текстовими повідомленнями.

Деякі з ознак, які допоможуть виявити соціальну інженерію:

1. Граматика і лексика. Зазвичай, зловмисники не приділяють увагу деталям та надсилають повідомлення з помилками, пропущеними словами та поганою граматикою. Ще один мовний елемент, який може сигналізувати про можливу атаку — це формальні привітання та фрази.

2. Адреса відправника. Більшість зловмисників не витрачають час на створення правдоподібного імені або домена відправника. Отже, якщо електронний лист надходить з адреси, яка є набором випадкових чисел та символів, або одержувач взагалі невідомий, варто перемістити цей лист до папки спам.

3. Почуття терміновості. Злочинці часто намагаються залякати жертв за допомогою фраз, які викликають тривогу, наприклад «терміново надішліть нам свої дані, або ваша посилка буде скасована» або «якщо ви не оновите свій профіль зараз, ми його видалимо». Банки, компанії з доставки, державні установи і навіть внутрішні відділи, зазвичай, спілкуються нейтрально і лише констатують факт. Тому, якщо у повідомленні намагаються змусити одержувача діяти дуже швидко, це може бути ознакою атаки.

4. Запит на конфіденційну інформацію. Офіційні установи та навіть відділи компанії, зазвичай, не вимагають надсилання конфіденційної інформації електронною поштою або телефоном, якщо про це попередньо не домовлялися.

5. Щось звучить занадто добре, щоб бути правдою. Це стосується розіграшів подарунків у соціальних мережах, а також електронних листів з унікальними та обмеженими пропозиціями.

Способи захисту закладу від атак з використанням соціальної інженерії:

1. Регулярне навчання з кібербезпеки усіх працівників. Таке навчання повинно показувати та моделювати випадки з реального життя, оскільки методи соціальної інженерії розраховані на користувачів з низьким рівнем обізнаності у кібербезпеці.

2. Здійснювати сканування на наявність слабких паролів, які потенційно можуть використати зловмисники для потрапляння до мережі вашого закладу. Крім того, створіть додатковий рівень захисту за допомогою двофакторної аутентифікації.

3. Впровадження рішення для захисту, які попереджають про можливі випадки шахрайства, а також повідомляють про виявлення спаму та фішингу.

4. Створення політики безпеки з чітким планом дій, які потрібно буде виконати працівникам, якщо вони стикнуться з проявами соціальної інженерії.

5. Використовувати рішення для централізованого управління корпоративною мережею, наприклад, ESET Security Management Center, щоб забезпечити повний огляд мережі, усіх рішень з безпеки та подій для виявлення та знешкодження потенційних загроз.

3. Онлайн (online) та офлайн (offline)-ідентифікація. Захист особистих даних.

Інтернет — це невід'ємна частина нашого життя. Він є глобальною системою взаємозалежних комп'ютерних мереж. Інтернет є мережею мереж, що дає можливість створення кіберпростору, де відбувається онлайнова комунікація. Кіберпростір ще називають віртуальною реальністю. Віртуальна реальність — це ілюзія дійсності, створена за допомогою комп'ютерних систем, які забезпечують зорові, звукові та інші органи чуття.

Чим більше часу ви проводите в Інтернеті, тим сильніше на ваше життя може вплинути ваша ідентичність як в Інтернеті, так і в офлайні.

Офлайн-ідентичність – це ви самі, особа, з якою ваші друзі та сім'я взаємодіють щодня вдома або на роботі. Оточуючі знають ваші персональні дані, а саме ваше ім'я, вік або місце проживання.

Ваша ідентичність в Інтернеті - це ви у кіберпросторі. Ваша ***онлайн-ідентичність*** – це те, як ви представляєте себе іншим в Інтернеті. Ця онлайн-ідентичність має розкривати лише мінімум інформації про вас.

Будьте обачні, обираючи ім'я користувача або псевдонім для себе в Інтернеті. Ім'я користувача не повинно містити жодної особистої інформації. Це має бути щось доречне і прийнятне. Ім'я користувача не повинно давати привід стороннім людям подумати, що ви є легкою ціллю для кіберзлочинців або хочете привернути небажану увагу.

У віртуальному світі Інтернету ми постійно стикаємося з проблемою забезпечення приватності. Згідно зі статтею 8 Європейської конвенції з прав людини, приватність закріплюється як окремий аспект приватного життя. Ніхто не має права збирати та поширювати інформацію про наше приватне життя. Особиста інформація, якою ми не хочемо ділитися, має залишатися конфіденційною, не підлягати розголосові. Питання збереження приватності в мережі Інтернет є актуальним, оскільки віртуальне спілкування практично ніколи не буває приватним. Інформація, що поширюється в режимі онлайн електронною поштою, соцмережами тощо легко може бути доступна іншим. Від неї також неможливо повністю позбутися. Недостатня захищеність інформації та своїх профілів

створює ризик доступу до неї інших людей і її використання без дозволу. Користувачі Інтернету самі несуть відповідальність за захист відомостей про своє життя.

Будь-яка інформація про вас може вважатися вашими персональними даними. Ця персональна інформація може однозначно ідентифікувати вас як особистість. Ці дані містять фото та повідомлення, якими ви обмінюєтесь з родичами та друзями в Інтернеті. Інша інформація, така як ім'я, номер соціального страхування, дата і місце народження або дівоче прізвище матері, відома лише вам і використовується для встановлення вашої особистості. Такі відомості, як медична, освітня, фінансова інформація та дані про працевлаштування також можуть бути використані для ідентифікації вас в Інтернеті.

Відповідно до Закону України «Про захист персональних даних»:

Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Зокрема, прізвище, ім’я, по батькові, адреса, телефони, паспортні дані, національність, освіта, сімейний стан, релігійні та світоглядні переконання, стан здоров’я, матеріальний стан, дата і місце народження, місце проживання та перебування тощо.

Незаконне отримання та оприлюднення (поширення) чужої особистої інформації є злочином. Підраховано, що кожна п'ята людина віком від 18 років ставала жертвою кібератаки в соціальних мережах або через мобільні пристрої. Найчастіше метою отримання особистих даних є доступом до банківських рахунках. Ваші дані в Інтернеті завжди мають певну цінність для кіберзлочинців.

Важливо! За порушення недоторканості приватного життя, а саме за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації винна особа притягується до кримінальної відповідальності (*стаття 182 Кримінального кодексу України*)

Комп'ютерні пристрої зберігають ваші дані та є порталом до вашого онлайн-життя. Навіщо та кому можуть знадобитися ваші особисті дані?

– Ними можуть скористатися рекламодавці (для збільшення кількості розсилок).

– Чужі особисті дані використовуються для отримання кредитів та крадіжок коштів із банків.

– Дані можуть бути викрадені з хуліганських спонукань (оприлюднити листування, наприклад).

– Дані можуть бути викрадені для подальшого перепродажу.

– Витік даних можливий з комп'ютера, ноутбука, мобільного пристрою. При цьому дані потрапляють до кіберзлочинців через Інтернет, електронну пошту.

– Цінність для зловмисників є і облікові записи електронної пошти. Адреса електронної пошти може бути використана для підтвердження реєстрації на інших веб-сайтах.

Цікаво, що поняття «витік персональних даних» в англійській мові відповідає Identity theft (крадіжка особистості).

Запровадження дистанційного навчання на початку пандемії спонукало педагогічних працівників швидко шукати способи, інструменти та електронні канали комунікації для його проведення і взаємодії з учнями та батьками.

Цифровізація освітнього процесу й робота з технологіями дистанційного навчання вже помітно вплинула на те, як відбувається освітній процес.

З одного боку значно розширилися і продовжують розширюватися можливості педагогів проводити навчання, а учнів – навчатися.

З іншого – використання цих методів, технологій та інструментів тісно пов’язане з безпекою роботи, зокрема, використанням та обробкою персональних даних учасників освітнього процесу.

Способи захисту особистих даних:

1. *Створення складних паролів*. Як правило, ми маємо більше ніж один обліковий запис в Інтернеті, і для кожного з них слід використовувати унікальний пароль. Таким чином, доводиться пам'ятати багато паролів. Проте, нехтування правилом використання сильних та унікальних паролів залишає дані вразливими для кіберзлочинців. Використання однакового пароля для усіх облікових записів в Інтернеті – це те саме, що й використання одного ключа для замикання усіх дверей. менеджери паролів допоможуть генерувати складні та унікальні паролі для кожного сайту та тримати їх в одному місці. Менеджери паролів допоможуть генерувати складні та унікальні паролі для кожного сайту та тримати їх в одному місці.

Менеджер паролів (1password, LastPass, KeePass) допомагає автоматично входити до облікових записів в Інтернеті, потрібно лише пам'ятати майстер-пароль, щоб отримати доступ до менеджера паролів і керувати всіма обліковими записами та паролями.

2. *Використання двофакторної аутентифікації.* Онлайн-сервіси, такі як Google, Facebook, Twitter, LinkedIn, Apple та Microsoft, використовують двофакторну аутентифікацію для забезпечення додаткового рівня захисту при вході до облікових записів. Крім імені користувача та пароля, або особистого ідентифікаційного номера (PIN) чи шаблону, для двофакторної аутентифікації іноді потрібен додатковий токен безпеки, такий як:

– Фізичний об'єкт - кредитна картка, телефон або ключ-брелок.

– Біометричне сканування - відбиток пальця, відбиток долоні, розпізнавання обличчя або голосу.

Навіть якщо використовується двофакторна аутентифікація хакери можуть отримати доступ до ваших облікових записів в Інтернеті через такі атаки, як фішинг, зловмисне програмне забезпечення та соціальна інженерія.

3. *Шифрування повідомлень*. Шифрування – це процес перетворення інформації у форму, в якій неавторизована сторона не зможе її прочитати. Більшість месенджерів вже використовують шифрування.

Наприклад, WhatsApp пропонує шифрування з 2016 року. Це означає, що ніхто не зможе побачити ваше повідомлення, окрім отримувача. Крім того – в месенджерах є секретні чати. Але експерти більше довіряють Telegram. А найзахищеніший і зовсім непопулярний в нас месенджер – Signal.

4. *Не підключатися до громадського WiFi.* Громадські мережі не завжди захищені паролем. Підключатись до відкритого WiFi – погана ідея. Хакери можуть створити мережу – двійника із такою ж назвою та перехопити дані.

Публічні Wi-Fi точки доступу (hot spot) дають змогу отримувати доступ до особистої онлайн-інформації та мандрувати Інтернетом. Тим не менш, краще не підключитися і не надсилати будь-яку важливу особисту інформацію через загальнодоступну бездротову мережу.

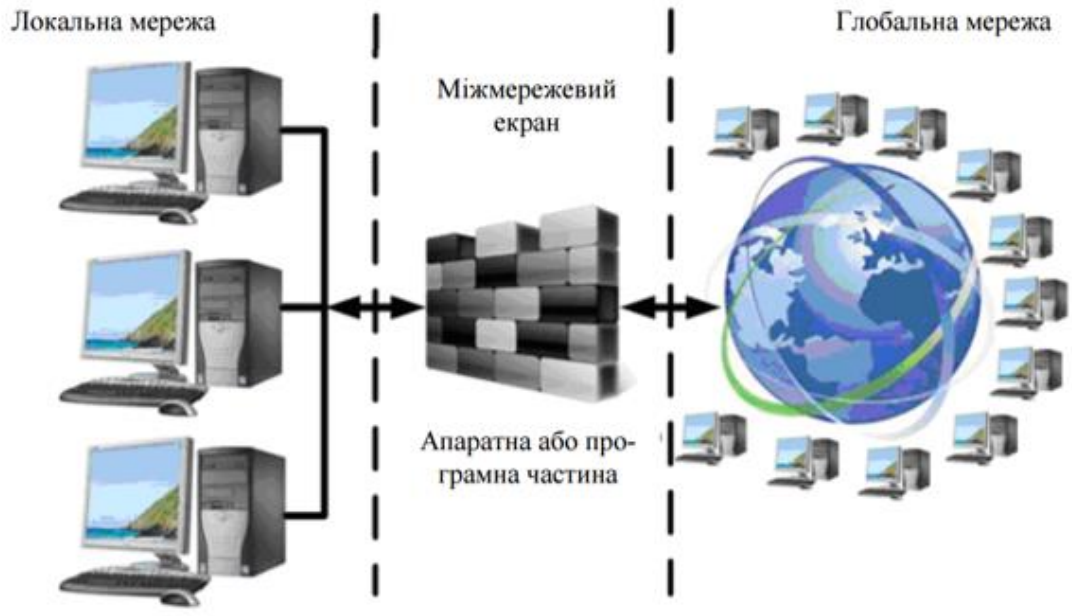
5. *Використання протоколу HTTPS.* Цей протокол більш безпечний, ніж HTTP, він шифрує всю інформацію та захищає від атак. Необхідно слідкувати, аби HTTPS обов’язково був в адресному рядку сайтів, де ми залишаємо дані банківської карти.

4. Захист організації.

Міжмережний екран (фаєрвол, брандмаурер) – це стіна або перегородка, яка призначена для запобігання поширенню вогню з однієї частини будівлі в іншу.

Міжмережевий екран (МЕ) виявляє та блокує мережевий трафік на основі попередньо визначених або динамічних правил. Вони захищають мережі та пристрої від вторгнення потенційно небезпечних кіберзлочинців, які можуть інфікувати пристрої та використовувати їх у зловмисних цілях.

МЕ служить захисною стіною між локальною мережею та зовнішньою мережею і запобігає будь-яким загрозам. Він призначений для контролю вхідного і вихідного трафіку на комп'ютері або в локальній мережі, дає змогу припиняти практично всі види мережевих атак, вирізати рекламу, відключати банери, рекламні скрипти, вспливаючі вікна та інше, не надсилати іншим «чужим» серверам інформацію про ваш комп'ютер, робить даремною роботу програм-троянів і засобів віддаленого адміністрування. Робота МЕ полягає в аналізі структури і вмісту інформаційних пакетів, що надходять із зовнішньої мережі, і в залежності від результатів аналізу пропускає пакети у внутрішню мережу (сегмент мережі) або повністю їх відфільтровує.



Головна функція брандмауера — фільтрація шкідливого та потенційно небезпечного контенту та з'єднань.

Розрізняють два типи МЕ: апаратний і програмний.

Апаратний являє собою пристрій, який фізично підключається до мережі. Цей пристрій відслідковує всі аспекти вхідного і вихідного обміну даними, а також перевіряє

адреси джерела і призначення кожного оброблюваного повідомлення, що забезпечує безпеку, допомагаючи запобігти небажаним проникненням в мережу або комп'ютер.

Програмний виконує ті ж функції, але використовує не зовнішній пристрій, а програмний продукт, який запущений на кінцевому комп'ютері або шлюзі. Найбільшого розповсюдження отримав програмний тип реалізації МЕ.

Існує кілька типів брандмауерів із різними видами фільтрування трафіку:

– Брандмауер першого покоління працює як *пакетний фільтр*, порівнюючи основну інформацію, таку як оригінальне джерело, призначення пакета, використовуваний порт чи протокол, з визначеним переліком правил.

– Друге покоління брандмауера містить ще один параметр для налаштувань фільтра — *стан з'єднання*. На основі цієї інформації технологія може відслідковувати дані про початок з'єднання та поточні з'єднання.

– Брандмауери третього покоління побудовані для фільтрування інформації за допомогою усіх рівнів моделі OSI, зокрема і *прикладного рівня*. Вони розпізнають програми та деякі широко поширені протоколи, такі як FTP та HTTP. На основі цієї інформації брандмауер може виявляти атаки, які намагаються обійти його через дозволений порт або несанкціоноване використання протоколу.

Нові фаєрволи все ще належать до третього покоління, однак їх часто називають *«наступним поколінням» або NGFW.* Даний вид поєднує всі раніше використані підходи з поглибленим оглядом відфільтрованого контенту та його порівнянням з базою даних для виявлення потенційно небезпечного трафіку.

Сучасні брандмауери часто мають вбудовані додаткові системи безпеки, наприклад віртуальні приватні мережі (VPN), системи запобігання та виявлення вторгнень (IPS/IDS), управління ідентифікацією, управління додатками та веб-фільтрація.

Переваги використання брандмауера: він забезпечує *покращення безпеки* та *захист пристроїв від шкідливого вхідного трафіку.*

Також технологія може фільтрувати вихідний трафік. Це допомагає зменшити ймовірність викрадення даних зловмисниками. Крім цього, важлива функція брандмауера полягає у зменшенні ризику пристроїв стати частиною ботнету — шкідлива мережа з великою групою пристроїв, що управляється кіберзлочинцями.

ПЛАНИ СЕМІНАРСЬКИХ ЗАНЯТЬ

Семінарське заняття 1

Тема 1. Поняття кібербезпеки. Он-лайн та оф-лайн ідентифікація. Методи та засоби захисту конфіденційної інформації, персональних даних учасників освітнього процесу (2 год)

Мета семінарського заняття: Допомогти педагогічним працівникам самостійно орієнтуватися в насиченому інформаційному просторі; розпізнавати маніпуляції та неправдиві дані, що поширюються через інтернет, соціальні медіа, месенджери; захищати власні персональні дані й протидіяти інформаційним загрозам; долучитися до інформаційної оборони України.

Дидактичні функції семінарського заняття

Навчальна: удосконалення знань щодо принципів безпечної роботи інформаційної системи, формування розуміння основ правових аспектів використання комп'ютерних програм та роботи в Інтернеті; вміння використовувати сучасні технології захисту інформації, вибирати засоби та інструменти захисту інформації, що мінімізують загрози несанкціонованого доступу до даних.

Професійна: удосконалення фахових компетенцій педагогічних працівників у сфері цифрових технологій, безпеки в Інтернеті, отримання практики розв’язання питань в основних напрямках кібербезпеки.

Комунікативна: розвивати вміння спілкуватися та вирішувати поставлені завдання.

Контролююча: виявлення рівня засвоєння знань з основ кібербезпеки в цифровому освітньому середовищі

Зміст семінарського заняття

1. Безпека браузерів. Найпоширеніші загрози та ризики для безпеки браузера
2. Безпечне користування месенджерами.
3. Безпечне користування електронною поштою. Аналіз повідомлень

Питання для обговорення

1. Поняття інформаційної безпеки і кібербезпеки
2. Найпоширеніші способи нелегального заробітку в мережі «Інтернет». Хакерські атаки.
3. Як працюють програми-вимагачі?
4. Cookie, призначення куків.
5. Найпоширеніші загрози та ризики для безпеки браузера. Як покращити безпеку браузера?
6. Безпека месенджерів. Які месенджери найбезпечніші?
7. Загрози під час користування поштовою скринькою. Легітимні та фішингові листи.

Теми доповідей

1. Сучасні методи технічного захисту інформації.
2. Основні положення Закону України «Про захист персональних даних».
3. Актуальність питання кібербезпеки на прикладі персональних даних.
4. Соціальні мережі з точки зору інформаційної безпеки.
5. Шахрайські дії в Інтернеті. Поняття кіберзлочинності.
6. Етика та безпека цифрової поведінки, цифрова репутація.
7. Електронні гроші. Безпека роботи з електронними грошима.
8. Публічні мережі. Безпека роботи в публічних мережах.
9. Методи забезпечення безпеки ПК та Інтернету. Віруси та антивіруси.
10. Види комп'ютерних злочинів. Причини поширення комп'ютерної злочинності.

Практичне завдання

1. Розробіть пам'ятку для своїх здобувачів освіти «Безпечне користування месенджерами».
2. Розробіть пам'ятку для своїх здобувачів освіти «Безпечне користування поштовою скринькою»
3. Розробіть пам'ятку для своїх здобувачів освіти «Як розпізнати фейк? Прості правила!»

Питання для самоконтролю

1.Під час зустрічі з адміністрацією училища представник приймальної комісії розглядає особливості майбутнього профорієнтаційного буклету, який буде випущений в наступному році:

☐ етично

☐ неетично

Обґрунтуйте _____

_____

_____

2. Ви розробили рекламу вашого закладу освіти з метою профорієнтаційної роботи. Співробітник вказує Вам на недоліки дизайну вашої реклами:

☐ етично

☐ неетично

Обґрунтуйте _____

_____

_____

3. Євгеній, ваш здобувач освіти, втратив свій учнівський квиток. Але через три дні він приймає участь у змаганнях, відстоює честь вашого закладу освіти і і не має часу чекати на виготовлення нового учнівського квитка, який потрібно пред'явити на змаганнях, щоб підтвердити, що Євген дійсно є учнем вашого закладу. Роман, його одногрупник, пропонує йому скористатися його учнівським. Чи етично це?

☐ етично

☐ неетично

Обґрунтуйте _____

_____

_____

Матеріал для опрацювання

1. Безпека браузерів. Найпоширеніші загрози та ризики для безпеки браузера

Доступ до мережі «Інтернет» став одним з основних прав людини. Ми користуємось мережею для дозвілля, розваги, роботи, а також забезпечення повсякденного буття – від оплати рахунків до замовлення послуг.

Вже залишився позаду той час, коли зловмисники використовували мережу лише для розваги або помсти. Зараз ціль будь-якого зловмисника-хакера – гроші. Кожного з них, перш за все, цікавить фінансова вигода. Тобто дії зловмисних програм, а також спеціальних шкідливих або зламаних чи скомпрометованих сайтів, спрямовані на те, щоб заробити на користувачі. А якщо на вас заробляють, то ви особисто обов'язково щось втратите: гроші, час, репутацію.

Найпоширеніші способи нелегального заробітку в мережі «Інтернет»:

– Програми-вимагачі – повністю або частково блокують ваш комп'ютер та вимагають оплату для розблокування.

– Викрадення облікових записів соціальних мереж «Фейсбук», «Твітер», «Інстаграм» тощо для розсилки спаму всім вашим друзям або шантажу з приводу повернення вашої сторінки.

– Викрадення поштових даних – як самої електронної скриньки, так і листів, що знаходяться на комп'ютері, в яких міститься інформація про ваші реєстраційні дані на інших ресурсах.

– Використання комп’ютера у складі bot-net – на тисячі комп’ютерів завантажуються шкідливе програмне забезпечення, яке застосовується для масової розсилки спам-повідомлень або для атаки інших ресурсів.

– Викрадення даних, які мають відношення до фінансових операцій: особиста документація, кредитні картки та інші платіжні системи.

– Несанкціонований показ рекламних повідомлень.

Проте що може статись, коли метою атаки є не людина, а інформаційна система міста, органу державної влади або іншої важливої установи? Насправді, людина стає тією ланкою, яка призводить не тільки до репутаційних та особистих майнових втрат, але й каталізатором критичних, а іноді й катастрофічних ситуацій.

Наприклад, у травні 2021 року одна з найбільших страхових компаній США CNA Financial Corp. заплатила наприкінці березня $40 млн, аби відновити контроль над своєю мережею після атаки хакерів. Компанія заплатила хакерам приблизно через два тижні після того, як було вкрадено цілу низку даних компанії, а доступ до мережі топменеджерам CNA було заблоковано. CNA спочатку ігнорувала вимоги хакерів, намагаючись відновити файли без взаємодії зі злочинцями. Але вже за тиждень компанія вирішила розпочати переговори з хакерами, які вимагали $60 млн.

Хакерська атака на лікарню міста Дюссельдорф призвела до смерті пацієнтки у вересні 2020 року. Жінку, якій знадобилася термінова госпіталізація, не прийняли в госпіталь через злам комп’ютерних систем і відправили в сусіднє місто Вуппераль, що знаходиться в 32 км. Через те, що час для порятунку було упущено, пацієнтка померла.

Що було причиною? В обох випадках першоджерелом атаки була помилка або недбалість посадової особи: від випадкового відкриття листа з шкідливим вкладенням до неналежного нагляду за програмним забезпеченням.

Яким чином це все відбувається? Наприклад, програма, яка була завантажена Вами з недостовірних джерел мережі «Інтернет» або запущена зі знайденого USB-носія, виходить у Всесвітню Мережу та завантажує троянську програму. Не одну. Зазвичай подібні загрози поширюються на комп'ютері як грибниця – там, де одна, там і інша. Цим самим зловмисники страхують себе від того, що існуючий антивірус зможе видалити всі небезпечні програми. Тож з великою вірогідністю один запуск програми-оманки – і 1-2-3-4 загрози залишаться на комп'ютері, як би Ви його не перевіряли, і будуть виконувати свою роботу, паралельно завантажуючи нових «братів» та активуючі необхідні функції.

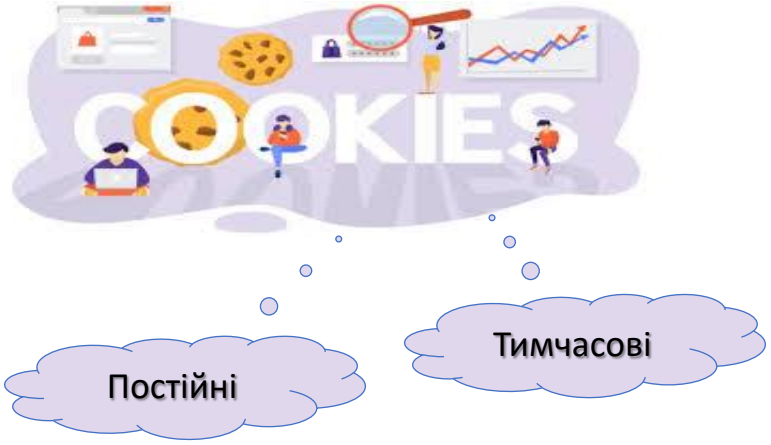
І це не обов'язково починається із завантаження підозрілої програми. Все може починатися інакше і «елегантно». Ви переглядаєте сторінки в інтернеті і в одну мить переходите за посиланням на небезпечний сайт або відомий сайт чомусь перенаправив вас на інший. З вигляду він може нічим не відрізнятися від інших сайтів і нести цікаву чи корисну інформацію – ніхто вас не попередить ні про загрозу, ні про її наслідки. Із сайту, використовуючи вразливості Вашого браузеру чи його додатків, на ваш комп'ютер без Вашої згоди (або взагалі інформування) таємно завантажується крихітна програма, яка у свою чергу скачує та інсталює вищезазначені загрози.

Браузер, Web browser – спеціальна програма, призначена для перегляду веб-сайтів. Основна мета інтернет-браузера – перевести код, за допомогою якого комп'ютери створюють веб-сайти, у текст, графіку та інші функції веб-сторінок, які ми звикли бачити сьогодні. Тобто, браузери транслюють код інтернет-сторінок у зрозумілий людині 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".

Через браузери користувачі отримують доступ у цифровий простір, де можна переглядати контент з усього світу. Зараз браузери також зберігають облікові дані, файли cookie, історії пошуку та іншу цінну інформацію про користувачів, яка може опинитися під прицілом кіберзлочинців.

Cookie — це невеликі текстові файли, які зберігаються в комп’ютері під час відвідування певних веб-сторінок.



Куки спрощують роботу в Інтернеті, зберігаючи потрібну інформацію. За допомогою файлів cookie сайти можуть запам'ятовувати ваш вхід в обліковий запис чи ваші уподобання, а також надавати вам персоналізований контент.

Файли cookie також можуть використовуватися для збору статистики про перегляд сторінок та показу цільових оголошень.

Cookies бувають тимчасовими і постійними. Постійні cookies залишаються на комп’ютері, коли ми закриваємо вкладку з сайтом, а тимчасові видаляються. Які саме cookies використовувати на конкретному сайті – тимчасові або постійні – вирішує його розробник. Саме тому на одних сайтах ми не виходимо з акаунтів, навіть коли заходимо на них раз через кілька днів, а на інших вводимо пароль заново, хоча відійшли від комп’ютера на п’ять хвилин.

Самі по собі cookies не є небезпечними – це звичайні текстові файли. Вони не можуть запускати процеси на комп’ютері та взагалі взаємодіяти з операційною системою.

Але їх можуть спробувати перехопити або вкрасти, щоб відстежити ваші попередні дії в мережі або входити у ваші акаунти без авторизації.

Зазвичай інформацію, яку записують в cookies, зашифровують перед відправкою, а самі cookies передають за HTTPS-протоколом. Це допомагає захистити призначені для користувача дані, але за впровадження шифрування і безпечну відправку відповідає розробник сайту. Відвідувачам залишається тільки сподіватися, що все налаштували грамотно. Зі свого боку користувач може тільки заборонити браузеру використовувати cookies або час від часу чистити їх самостійно.

Зовсім відключати cookies – не завжди хороша ідея. Наприклад, всі інтернет-магазини працюють за допомогою cookies. Якщо заборонити браузеру їх використовувати, сервер не зможе запам’ятати, що саме ви додали в кошик. Чистити cookies вручну

практичніше, але доведеться щоразу заново налаштовувати зовнішній вигляд сайту і входити в акаунти.

Найпоширеніші загрози та ризики для безпеки браузера:

1. Наявність вразливостей. Через те, що користувачі часто нехтують застосуванням регулярних оновлень, браузер та встановлені плагіни чи розширення можуть містити уразливості. Їх зловмисники використовують для викрадення конфіденційних даних або завантаження шкідливого програмного забезпечення. Атаки часто починаються з фішингового електронного листа чи повідомлення або відвідування інфікованого сайту зі шкідливою програмою, а також завантаження небезпечного файлу.

2. Використання програм. Зловмисники націлені на програми на комп'ютері, а браузер при цьому використовується для доставки або виконання шкідливого компоненту. Серед найвідоміших форм — трояни, програми-вимагачі, віруси, черв'яки та банківські шкідливі програми. Об'єднує всі ці види шкідливих програм — зловмисні наміри їх авторів чи операторів.

3. Шкідливі плагіни.

Плагін – це програма, які полегшує користування мережею «Інтернет».

Існують тисячі плагінів, які користувачі можуть завантажити, щоб покращити роботу в Інтернеті. Однак багато з них мають привілейований доступ у браузері. Це означає, що зловмисники можуть замаскувати шкідливі плагіни під легітимні та використовувати їх для викрадення даних та завантаження небезпечного програмного забезпечення.

4. Атаки «людина посередині». Під час цього виду атаки зловмисник може змінити трафік, наприклад, переспрямувати жертву на фішингову сторінку, завантажити програму-вимагач або викрасти облікові дані. Такий ризик зростає під час використання публічних мереж Wi-Fi.

5. Інфікування системи доменних імен (DNS).

DNS — це адресна книга Інтернета, яка перетворює введені доменні імена на IP-адреси для відображення у браузері сайтів.

Однак атаки на систему доменних імен, які зберігаються на комп'ютері, або на самі DNS-сервери можуть дозволити зловмисникам перенаправляти браузери користувачів на шкідливі домени, зокрема фішингові сайти.

6. Перехоплення сеансу. Більшість веб-сайтів використовують ідентифікатори сеансу під час входу користувачів. Якщо зловмисникам вдасться зламати чи перехопити ці ідентифікатори (у разі відсутності шифрування), кіберзлочинці можуть увійти на ті самі

сайти чи у програми під виглядом користувача. У такому випадку можна швидко викрасти конфіденційні дані та фінансову інформацію.

Чому через браузер можуть реалізовуватись загрози?

– Браузери застарівають та з'являються вразливості, які експлуатуються хакерами віддалено.

– Хакери зламують легітимні сайти та розміщують на них шкідливий код та програми, і Ви можете навіть не знати про те, що стали жертвою.

– Зловмисники зламують публічні точки доступу до мережі «Інтернет» і намагаються перехопити інформацію користувачів.

Як покращити безпеку браузера?

Щоб запобігти потенційним загрозам для безпеки браузера та конфіденційних даних під час перегляду веб-сторінок, варто дотримуватись наступних порад.

1. Оновлюйте браузер та встановлені плагіни, щоб мінімізувати шанси використання вразливостей, а також видаліть усі застарілі плагіни.

2. Відвідуйте лише безпечні сайти з використанням протоколу HTTPS, про що свідчить замок в адресному рядку. У такому випадку хакери не зможуть перехопити трафік з браузера до веб-сервера.

3. Остерігайтесь фішингових загроз, які поширюються через електронну пошту та онлайн-повідомлення. Ніколи не відповідайте на небажані електронні листи, не перевіривши дані відправника, та не надсилайте конфіденційну інформацію незнайомцям.

4. Не завантажуйте підозрілі програми чи файли, а у випадку потреби використовуйте для цього виключно офіційні ресурси.

5. Використовуйте багатофакторну автентифікацію, щоб зменшити ризики викрадення облікових даних.

6. Застосовуйте VPN від надійного провайдера, а не безкоштовну версію. Це створить зашифрований тунель для Інтернет-трафіку та захистить від відстеження сторонніми особами.

VPN або «віртуальна приватна мережа» – це сервіс, який захищає ваше інтернет-з'єднання і конфіденційність в Інтернеті. Підключення до VPN-мережі робить вашу IP-адресу майже невидимою. Зокрема VPN переносить ваше з'єднання на сервер у країні, яку ви оберете, і показує IP-адресу з того місця.

Таким чином, VPN працює як додатковий рівень захисту, шифруючи всі дані, які проходять через неї, та забезпечуючи конфіденційність в Інтернеті. Особиста інформація, дані місцезнаходження та історія веб-перегляду будуть недоступними для прочитання тим, хто спробує вас ідентифікувати та відстежити. Навіть ваш Інтернет-провайдер не зможе збирати дані про вас.

Під час використання загальнодоступного Wi-Fi ви підключаєтеся до менш безпечної мережі, створюючи ідеальну можливість для хакерів отримати доступ до ваших пристроїв. Використання VPN-мережі допоможе зашифрувати з'єднання та захистити вас від зловмисників, які хочуть викрасти особисту інформацію, паролі чи банківські реквізити.

7. Завантажуйте багаторівневе рішення для захисту комп'ютерів та мобільних пристроїв від різних онлайн-загроз.

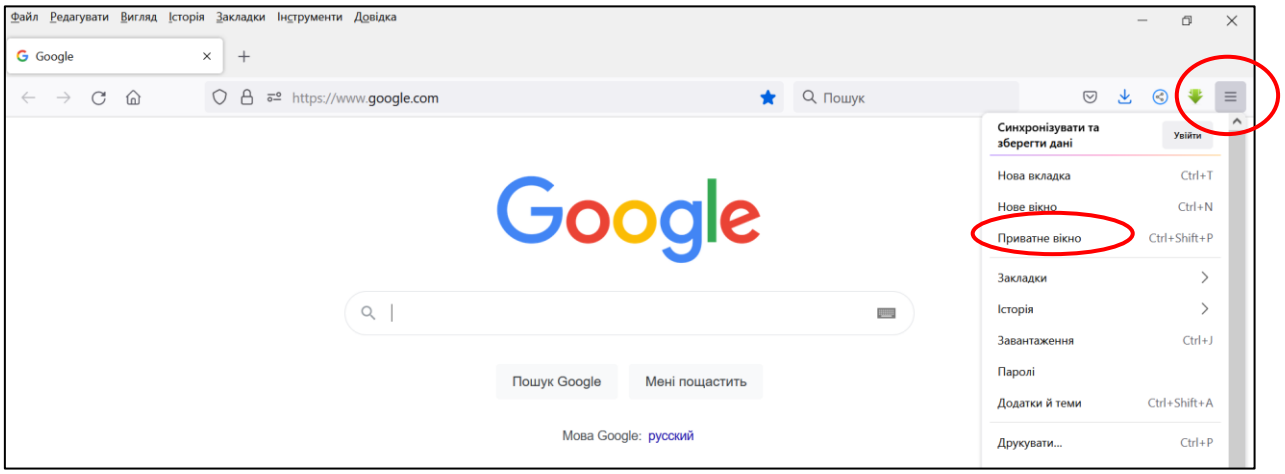
8. Увімкніть автоматичні оновлення операційної системи та програмного забезпечення на пристрої.

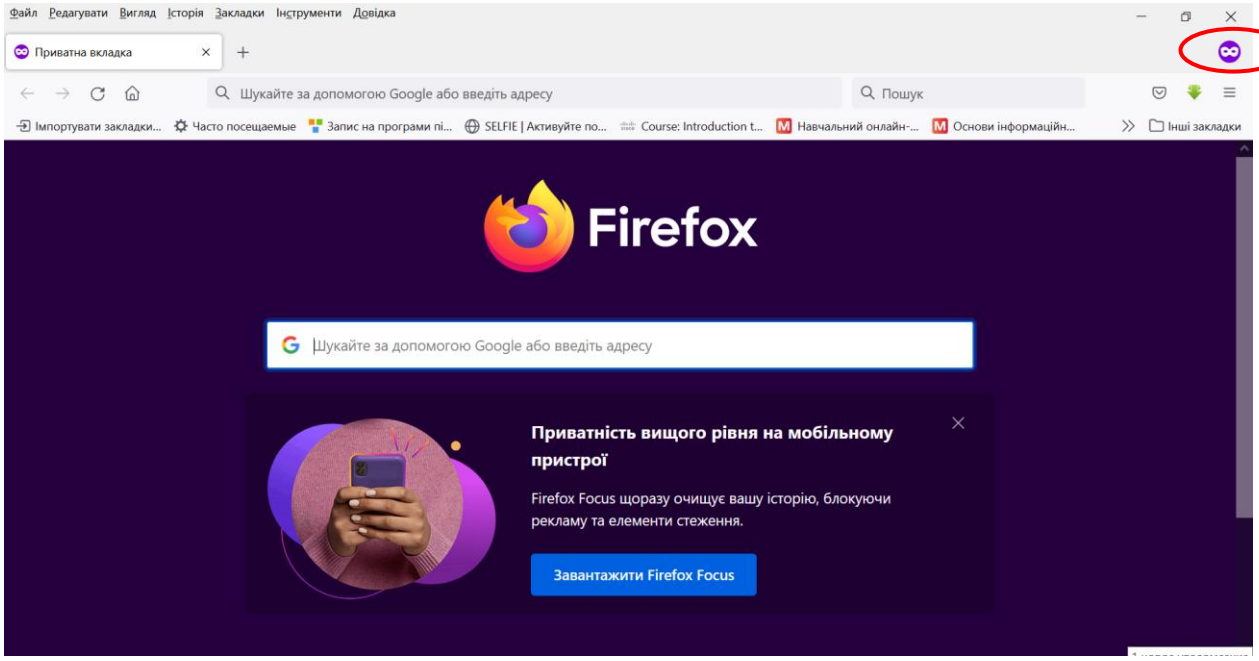
9. Перегляньте налаштування конфіденційності та безпеки браузера, щоб запобігти відстеженню та заблокувати сторонні файли cookie і спливаючі вікна.

10. Вимкніть автоматичне збереження пароля в браузері.

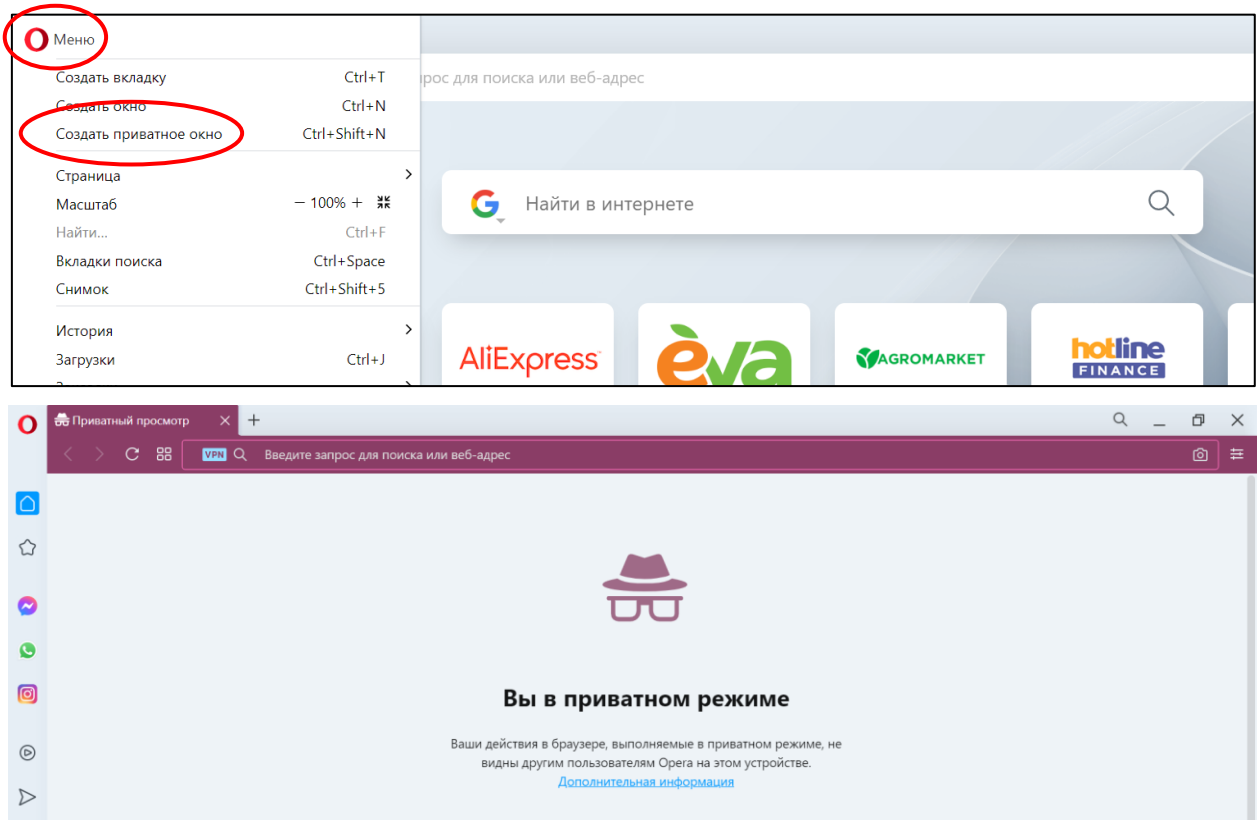
11. Використовуйте параметри приватного перегляду, щоб запобігти відстеженню файлів cookie.

Приватний перегляд - використання Firefox без збереження історії

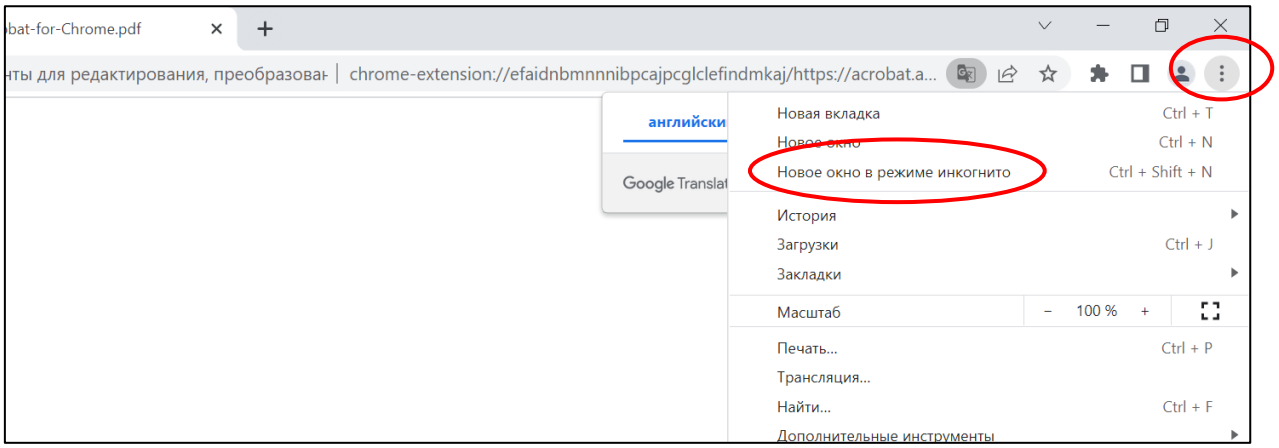


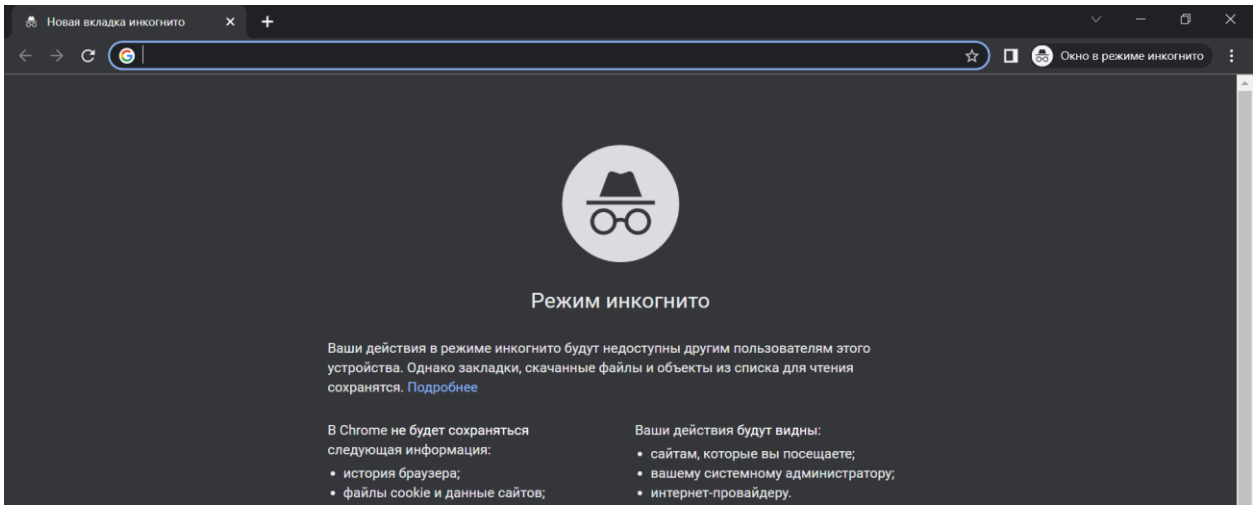


Приватний перегляд - використання Opera без збереження історії



Приватний перегляд - використання Opera без збереження історії





2. Безпечне користування месенджерами.

У перекладі з англійської «messenger» означає «гонець», «посланник», «посланець». Словом, «той, хто приносить новини».

Месенджер – це спеціальний додаток або програма, яку завантажують і встановлюють на смартфон або комп'ютер. Його основна мета - це миттєвий обмін текстовими повідомленнями, фото, картинками, відео, документами з друзями, родичами, знайомими, колегами по роботі або по навчанню. Також можна здійснювати дзвінки за допомогою аудіо або відеозв'язку.

Які ризики несе користування месенджерами?

1. Розкриття вашої приватної інформації: від номеру телефону до фотографій.

2. Шахрайство – шахраї дуже часто користуються саме месенджерами, щоб уникнути виявлення.

3. Розповсюдження шкідливого ПЗ через функції автозавантаження.

У 2017 році була виявлена тенденція – викрадення інформації через месенджери.

У 2018 році кількість витоків інформації через месенджери зросла на 14,3%, хоча раніше цей канал зовсім не виділявся в статистиці. Крім того, постійно виявляються нові модифікації шкідливих програм, що відстежують переписку в популярних месенджерах.

У мирний час наше спілкування переважно відбувалася онлайн у різних месенджерах. А відколи розпочалася повномасштабна війна, і поготів – смартфони не випускаємо з рук. Але війна нині триває і у кіберпросторі – ворог намагається заволодіти нашою інформацією.

Якими месенджерами користуватися зараз найбезпечніше?

Telegram

Раніше популярний здебільшого серед молоді, після 24 лютого Telegram перетворився у найоперативніший канал для повідомлення інформації. Новинні Telegram-канали набирають сотні тисяч підписників, свої канали для швидкого транслювання офіційної інформації створили державні органи, нардепи, чиновники.

Ще від початку роботи месенджера в Україні, довкола нього виникало багато підозр. Засновник Telegram – Павло Дуров, той, що придумав популярну в Росії мережу *ВКонтакте*. Скептики підозрювали, що Telegram зливає конфіденційну інформацію українських користувачів російській ФСБ. Відповідні пересторогиви никли знову, коли Росія розпочала повномасштабну війну в Україні.

Сам Дуров написав, що має родичів в Україні, і те, що відбувається, його особиста трагедія. Він нагадав, як закінчилася його кар'єра у Росії, мовляв, 2013 року російська ФСБ вимагала керівництво ВКонтакте надати їм особисті дані українських користувачів ВК, які протестували проти президента-втікача. Дуров відмовився це зробити, і його звільнили з його ж компанії. Він більше не живе в Росії, не має там ані бізнесу, ані співробітників. І, мовляв, приватність усіх користувачів Telegram – священна.

За останні роки Telegram зарекомендував себе як досить практичний і захищений месенджер, віднедавна орієнтований на групові аудіо- та відеодзвінки.

Одна з головних переваг Telegram з погляду безпеки — можливість використовувати «секретні чати», які захищені наскрізним шифруванням. У секретних чатах також можна налаштувати період автоматичного видалення всіх повідомлень.

За замовчуванням у Telegram встановлено двофакторну автентифікацію та власний алгоритм шифрування MTProto, який дозволяє об'єднати відразу кілька популярних протоколів безпеки (AES; RSA та протокол обміну ключами Діффі-Геллмана).

Кілька місяців тому засновник «сек'юрного» месенджера Signal Моксі Марлінспайк розкритикував Telegram і заявив, що цей сервіс нічим не відрізняється від месенджера Facebook.

«Мене дивує, що після всього часу майже всі ЗМІ, як і раніше, називають Telegram „зашифрованим месенджером". Telegram має безліч привабливих функцій, але з погляду конфіденційності та збору даних найгіршого вибору немає», — написав Марлінспайк у Twitter.

Головною проблемою Telegram засновник Signal вважає те, що месенджер зберігає всі дані користувачів на своїх серверах, і в разі атаки хакера особиста інформація може потрапити до рук зловмисників.

Засновник Telegram Павло Дуров відповів на цю заяву тим, що навіть «безпечні» месенджери на кшталт Signal спочатку фінансувала влада США, не кажучи вже про WhatsApp, який постійно передає дані користувачів третім сторонам.

«Я чув, що наші американські конкуренти розчаровані тим, що вони не можуть зрівнятися зі зростанням Telegram, незважаючи на значні інвестиції у маркетинг (те, у що Telegram ніколи не доводилося інвестувати). Але щоб відповідати нашому зростанню, вони повинні спочатку переконатися, що їхні дії відповідають їхнім маркетинговим заявам. До того часу витік даних і проблеми з безпекою в їхніх застосунках, на жаль, залишаться неминучими», — написав Дуров.

Facebook Messenger

Месенджер від Facebook – другий в Україні за популярністю серед користувачів. Утім, щодо його безпечності думки різняться. У деяких експертів виникають пересторороги, яким чином велика соціальна мережа може використовувати особисті дані користувачів. Особливо з огляду на те, що Facebook фігурував у схожих скандалах. Проте фахівець з кібербезпеки Костянтин Корсун цей месенджер називає непоганим.

«*Непогано захищений месенджер Facebook, питання лише до того, чи використовує компанія Facebook ваші дані у своїх рекламних цілях. Але це не росіяни. Це американці, у них діють закони, діють правила», – переконаний експерт.*

WhatsApp

Месенджер, який також наразі належить компанії Facebook. На офіційному сайті розробники запевняють, що WhatsApp має наскрізне шифрування, відтак можна без жодних побоювань ділитися зі співрозмовниками особистою інформацією. Повідомлення зберігаються на пристроях користувачів, а не на серверах компанії. Утім, неодноразово WhatsApp потрапляв у різні скандали, пов'язані зі збереженням приватності. І навіть стеженні за користувачами.

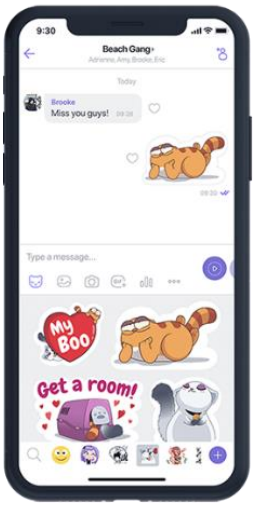
На початку 2021 року месенджер оновив правила конфіденційності, попередивши, що може обмінюватися даними з мережею Facebook, якій він належить. Багато користувачів таку політику розкритикували та перейшли в інші месенджери.

У WhatsApp наскрізне шифрування працює за замовчуванням, можна включити двофакторну автентифікацію і налаштувати обмежений доступ до програми.

Головні мінуси цього сервісу — відсутність секретних чатів, зберігання інформації на пристроях у відкритому вигляді та використання хмарних сховищ для даних резервного копіювання.

В іншому ж до безпеки платформи виникає не більше запитань, ніж до її конкурентів.

Viber



Найпопулярніший месенджер в Україні. Viber пропонує своїм користувачам наскрізне шифрування, секретні чати з функціями автоматичного видалення повідомлень, заборони або відстеження скріншотів, а також захисту від копіювання та пересилань повідомлень.

На відміну від Telegram, у Viber повне шифрування за замовчуванням увімкнено для всіх чатів, але, як і Telegram, всі резервні копії чатів тут зберігаються у відкритому вигляді.

Крім цього, кілька років тому повідомляли, що деякі сервери компанії розміщуються на території Росії і немає гарантії, що спецслужби цієї країни не мають доступу до переписки користувачів.

«Безпечні» месенджери

Окрему категорію сервісів швидких повідомлень становлять так звані «сек'юрні» месенджери, які акцентують увагу на безпеці своїх послуг і захищеності даних користувачів.

Один із найпопулярніших таких месенджерів (принаймні в нашій країні) — згаданий вище Signal. Багато експертів називають криптографічний протокол Signal «еталоном для індустрії».

Всі чати в цьому месенджері зашифровані за замовчуванням, і, як передбачається, навіть творці програми не можуть отримати доступ до ваших даних.

Головною проблемою месенджера залишається відсутність популярних у Telegram, Viber і WhatsApp функцій, а також низька популярність Signal серед користувачів, далеких від поняття «кібербезпека».

Застосунок Signal для смартфона, а також його ПК-версію можна завантажити безкоштовно. І за нинішніх умов було б не зайвим це зробити.

Серед інших «сек'юрних» месенджерів варто виділити сервіси Threema, Briar, Zello, тощо. Подібні програми досить специфічні у використанні, підходять не для всіх пристроїв і деякі функції можуть бути платними.

З огляду на те, що в нашій країні далеко не всі користувачі звикли платити за будь-яке ПЗ — саме Signal може стати оптимальним варіантом для тих, хто раптово вирішив подбати про безпеку свого цифрового спілкування.

До речі, нещодавно у Мережі писали про злам месенджера Signal, але Державна служба спеціального зв'язку та захисту інформації України спростувала цю інформацію.

Висновок. Назвати однозначно «безпечний» месенджер — неможливо. Будь-який онлайн-сервіс може зазнати хакерських атак, унаслідок яких ваші дані можуть потрапити до рук зловмисників.

Але загроза кібератак, що зросла, після вторгнення РФ в Україну — це найкращий час для виконання всіх правил інформаційної безпеки в месенджерах.

Як користуватися месенджерами безпечно?

Центр протидії дезінформації при РНБО України розробив коротку інструкцію для користувачів месенджерів. Її радять дотримуватися завжди, а особливо у воєнний час, коли ворог полює і на нашу особисту інформацію.

1. Оновлюйте месенджери.

2. Не передавайте через месенджер жодну інформацію, розкриття якої для вас небажане.

3. Відключайте автоматичне завантаження файлів, особливо для контактів, що відсутні у вашій адресній книзі.

4. Не переходьте за посиланнями, особливо скороченими, які надійшли від недовірених контактів.

5. Використовуйте “зникаючі” повідомлення, або “одноразовий перегляд”.

6. Активуйте двофакторну аутентифікацію, щоб додатково захистити свій обліковий запис.

7. Налаштуйте “конфіденційність”, щоб контролювати, хто може бачити вашу фотографію і додавати до груп.

8. Перегляньте історію чату та членство в групах. За можливості очищайте історію чату.

9. Надсилайте скарги на будь-які контакти, які здаються вам шахрайськими, розсилають погрози або інші небезпечні повідомлення.

Пам’ятайте про основне: Ваша особиста безпека – це Ваша відповідальність. Але від Вашої безпеки може залежати добробут та майбутнє співробітників, близьких та інших громадян України.

3. Безпечне користування електронною поштою. Аналіз змісту повідомлень

Кожного дня ми використовуємо електронну пошту для робочих та особистих цілей. Вона стала одним з основних каналів комунікації з нами і тому є неабияк привабливою для кіберзлочинців та інших зацікавлених сторін.

Після того, як люди почали активно користуватись емейлом, історія бачила чимало успішних кібератак, які використовували пошту як інструмент доставки шкідливого програмного забезпечення та виманювання у людей конфіденційної інформації.

Фішинг – атака, яка в основному використовує електронну пошту як вектор і обманом змушує людей завантажувати шкідливі програми собі на пристрої. Близько 60% підприємств зіткнулися з фішингом в 2021 році.

У 2020 році було багато фішингових електронних листів, пов'язаних з COVID-19. Шахраї розсилали інформацію від імені Всесвітньої організації охорони здоров'я, граючи на страху осіб.

Чому електронна пошта настільки приваблива для кіберзлочинців?

– Бази даних поштових скриньок легко знайти в мережі «Інтернет»;

– Функція додатків до листів дозволяє злочинцям надсилати файли з шкідливим програмним кодом;

– Користувачі не очікують отримати листи зі шкідливими вмістом/ Користувачі часто несвідомо відкривають всі листи, які до них надходять;

– Злочинці користуються людською психологію, щоб збільшити шанси відкриття шкідливих файлів (наприклад маскуючись під…).

Одним з перших правил безпеки електронної скриньки є чітке розмежування особистої та службової пошти.

Службова пошта:

– показує вашу належність до організації – (vasyl@me.gov.ua). Ми бачимо, що Василь належить до Міністерства розвитку економіки. Тим самим викликає довіру та авторитет до листів, які надходять з цієї адреси;

– дані зберігаються на серверах вашої установи і адмініструються відділом інформаційних технологій. Треті сторони не повинні мати доступ до цих даних;

– містить конфіденційну інформацію, яка стосується вашої організації.

Особиста пошта:

– зберігається на серверах компанії, яка надає послуги поштового сервісу;

– містить вашу приватну інформацію;

– використовується для реєстрації у соціальних мережах та на інших ресурсах.

Які загрози існують під час користування поштовою скринькою?

Фішинг з метою

– виманити ваші конфіденційні дані;

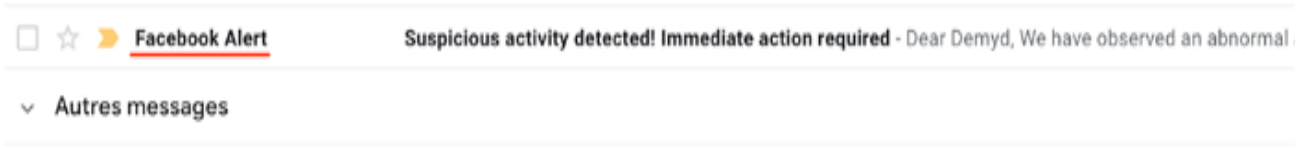
– зараження системи/мережі організації з метою паралізації всієї системи (шифрування вашого комп’ютера);

– отримання віддаленого доступу до комп’ютера та, як наслідок, мережі

Як відрізняти легітимні листи від фішингових (investigation)?

Вам надійшов лист. Ви очікували на нього? Ні? Проведімо аналіз метаданих:

1. Спершу, ми подивимось, хто відправник. Ви знаєте його? Вважайте, ім'я відправника можна поставити будь-яке.



2. Яка тематика повідомлення? Якщо вона викликає якусь квапливість або кличе до швидкої дії, це має бути індикатором, що до листа треба поставитись серйозно та обережно. *Приклад*: «Вас зламали! Швидше поміняйте пароль».

3. Коли ви відкрили лист, зверніть увагу на правильність написання домену відправника. Кіберзлочинці часто підмінюють літери/символи, щоб замаскуватись під авторитетне джерело.

В період президентських виборів у США 2016 року для проведення фішинг-атаки на базі схожих доменів зловмисники використали сайт «accountsgoogle.com» як клону сайту «accounts.google.com».

Коли ми переконались, що лист надійшов саме з достовірної адреси, ми можемо проаналізувати зміст повідомлення.

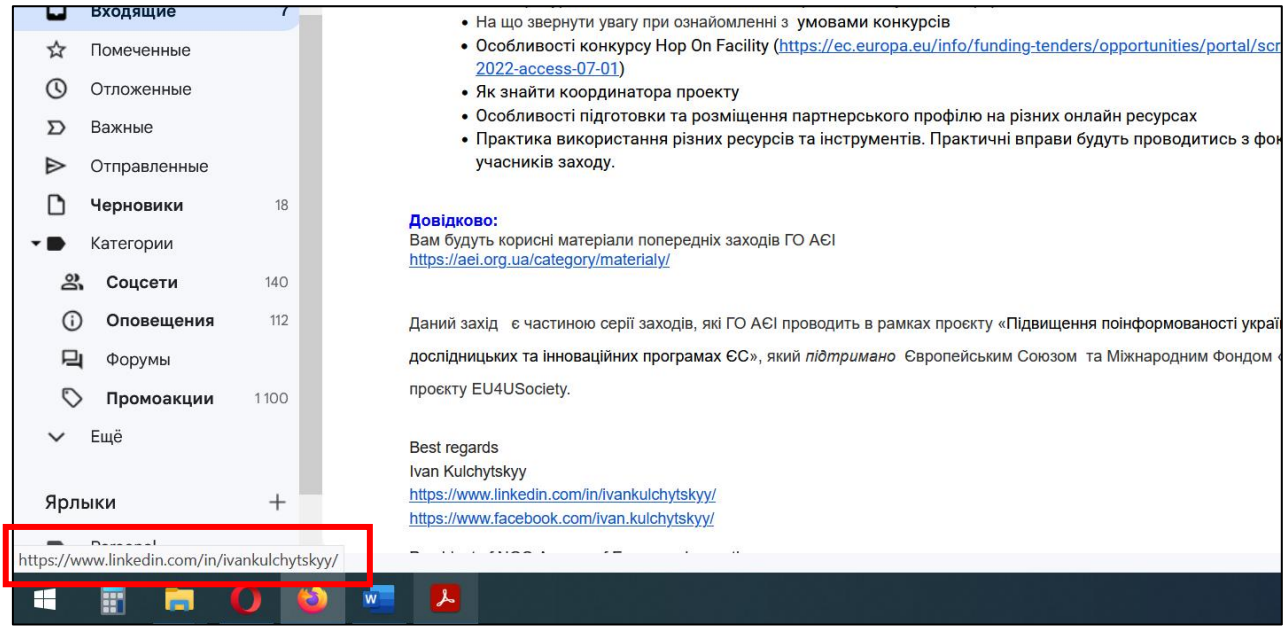
Аналіз змісту повідомлення.

1. Перше на що варто звернути увагу: чи звертаються до вас на ім'я? Чи використовують загальні фрази «Шановні колеги», «Шановний клієнте» і тд. Злочинець може вказати ваше ім'я, тоді атаку можна вважати підготовленною спеціально під вас.

2. Наступний індикатор фішингового листа – мова та наявність граматичних/орфографічних помилок. Наприклад, "Google" надсилає листи, які стосуються облікового запису, мовою інтерфейсу цього запису. Тобто, якщо у вас інтерфейс українською мовою, а лист прийшов російською, це серйозна причина задуматися.

3. Якщо ви отримуєте файл у додатку та пароль для відкриття його, це є великою підозрою на наявність у ньому шкідливого коду. Чому? Справа в тому, що у поштових сервісів є свої антивіруси, які сканують файли на наявність вірусів. Злочинці про це також знають, тому використовують функціонал архіваторів (WinRar, ZIP, та інші), щоб зашифрувати вміст файлу паролем. Таким чином, коли ви отримуєте файл на пошту, поштовий антивірус не може розпізнати шкідливість файлу, оскільки він зашифрований.

4. Далі, подивімось чи є якісь активні посилання у листі? Спробуйте навести мишкою на посилання (не натискаючи) та потримайте декілька секунд. У лівому нижньому куті, подивіться, куди насправді воно вас веде.



Важливо!!! *Посилання такого вигляду*

accounts.google.com.evilwebsite.pe/EditPasswd

шахрайське, бо адреса має починатися з accounts.google.com/ (тобто, після.com мусить бути /, а не крапка).

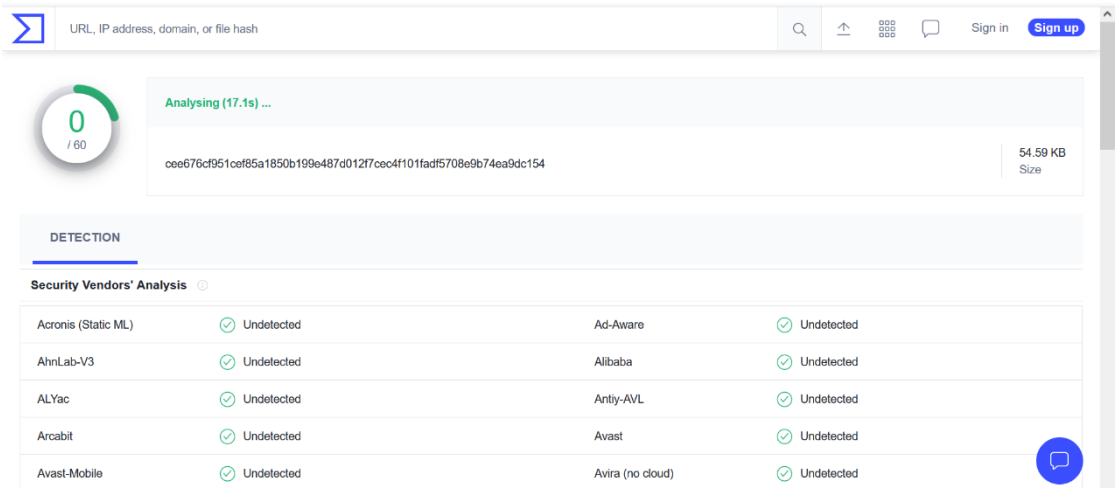
Як убезпечити свою поштову скриньку?

1. Використовувати складний пароль. Складний пароль – той, який містить в собі літери, символи та цифри і за довжиною не менше 8 символів. Пароль не повинен містити слів, які можна знайти у словнику.

Приклад поганого паролю: rockandroll123

Приклад надійного паролю: T@8l3S0bk4hA7

2. Не передавайте нікому свої паролі
3. Встановити 2-ий фактор аутентифікації
4. Ніколи не відкривати файли, не переконавшись у їхньому походженні. Використовувати додатковий канал комунікації, аби перевірити, чи дійсно надсилали вам цей лист (наприклад, за допомогою телефону, месенджеру і тд.).
5. Не використовувати службову пошту в особистих цілях.
6. Маєте сумніви щодо походження файлу, використовуйте https://virustotal.com для сканування файлу 50-ма антивірусними програмами.



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

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

Якщо так сталося, що Ви перейшли за посиланням у фішинговому листі, тоді:

1. Треба якомога швидше змінити пароль;
2. Продивитися відкриті сесії та закрити ті, які тобі не належать;
3. Повідом про це IT-відділ.

Якщо відкрив файл у додатку і зрозумів/ла, що це був фішинг, тоді:

1. Вимкнути комп'ютер;
2. Звернитися до відділу IT-технологій.

Семінарське заняття 2

Тема 2. Забезпечення інформаційної безпеки учасників освітнього процесу в ЗП(ПТ)О (2 год.)

Мета семінарського заняття: підвищення рівня професійної компетентності щодо правильного поводження з інформацією у кіберсфері та безпечної роботи із засобами комп'ютерної техніки в освітньому середовищі.

Дидактичні функції семінарського заняття

Навчальна: формування розуміння основ положень та термінів, що стосуються кібергігієни на робочу місці, основ нормативно-правової бази у сфері кібербезпеки та інформаційної безпеки, заходів кібергігієни на робочої місці. Набуття навичок визначати заходи кібергігієни для конкретної ситуації, оцінювати загрози та вживати заходів реагування на робочому місці

Професійна: удосконалення навичок організації безпечного доступу до пристроїв і програм, критичного оцінювання інформації, отримання практики розв'язання питань в основних напрямках кібербезпеки, безпечно поводитись у кіберсфері.

Комунікативна: розвивати вміння спілкуватися та вирішувати поставлені завдання.

Контролююча: виявлення рівня засвоєння знань з основ кібербезпеки та кібергігієни.

Зміст семінарського заняття

1. Онлайн-середовище та безпека. Кібергігієна.
2. Документи, що регламентують роботу закладу освіти з персональними даними під час дистанційного навчання.
3. Дії закладу освіти задля безпеки дистанційного навчання.
4. Рекомендації педагогічним працівникам для безпеки дистанційного навчання.
5. Рекомендації для батьків.
6. Правила інформаційної війни: як не нашкодити і бути корисним в Інтернеті.

Питання для обговорення

1. Що відносять до персональних даних? Як поясните здобувачу освіти необхідність захисту чи обмеження доступу сторонніх осіб до її персональних даних?
2. Як викладачу забезпечити захист персональних даних під час дистанційного навчання?

3. Захист персональних даних під час спілкування в соціальних мережах
4. Способи отримання електронного підпису.
5. Розпізнаємо фейк

Теми доповідей

1. Безпечне користування електронною поштою
2. Шкідливе програмне забезпечення
3. Безпека користування соціальними мережами
4. Безпека мобільних пристроїв
5. Фізична безпека
6. Убезпечення від неправдивих повідомлень
7. Правові засади кібергігієни

Практичне завдання

1. Підготуйте презентацію на тему «Кібербулінг — ідентифікація та запобігання».
2. Підготуйте презентацію на тему «Мобільні додатки батьківського контролю».
3. Підготуйте презентацію на тему «Рекомендації для учасників освітнього процесу щодо організації роботи за комп'ютером без шкоди для здоров'я».

Тестовий контроль знань

1. Вішинг – це:

- Різновид фішингу, який здійснюється через телефон
- Вид фішингового електронного листа
- Вид шкідливого програмного забезпечення
- Програмний комплекс для захисту від фішингових атак

2. Чому атаки з використанням прийомів соціальної інженерії до сьогодні залишаються одним із найефективніших методів атак?

- Вони дешеві в проведенні
- Незважаючи на відносну простоту в здійсненні, вони відрізняються високою ефективністю

- Соціальна інженерія атакує не операційну систему та не програмне забезпечення, а їхнього користувача, який найчастіше є найвразливішим
- Усе перераховане вище

3. Що із перерахованого нижче, на вашу думку, є найціннішим для хакера при плануванні фішингової атаки на підприємство, державну структуру? (Виберіть два варіанти)

- Фізична адреса головного офісу
- Інформація щодо структури внутрішньої мережі
- Інформація щодо контрагентів, партнерів, підрядників
- Ім’я керівника

4. Чи безпечно передавати дружині/чоловіку номер картки через WhatsApp? Адже цей месенджер шифрує дані при передачі!

- Так
- Ні, бо є інші ризики

5. Під час вихідних ви часто відвідуєте своє улюблене кафе та користуєтесь мережею Інтернет, під’єднуючись до загальнодоступного Wi-Fi. Що ви маєте пам’ятати?

- Небезпечно використовувати будь-які фінансові інтернет-сервіси із загальнодоступних мереж
- Легше і простіше користуватися загальнодоступними мережами Wi-Fi, які не вимагають пароля
- Якщо доступно кілька загальнодоступних мереж Wi-Fi, краще використовувати мережу з найкоротшим ім’ям

6. Що є найнадійнішим засобом забезпечення безпеки інтернет-браузера?

- Постійні оновлення
- Встановлення антивірусу
- Встановлення додаткових плагінів

7. Ви переглядаєте сайти в мережі Інтернет, аж раптом з’являється підозріле оголошення, на яке ви не очікували. Тут ви зрозуміли, що маєте використовувати блокатори реклами. Які причини є для цього з погляду кібербезпеки? (Виберіть два варіанти)

- Оголошення відволікають і дратують
- Оголошення можуть містити фішинг-посилання
- Оголошення часто рекламують зміїну олію
- Оголошення можуть призвести до завантаження вірусів

8. Що може мати на меті злочинець, надсилаючи фішинговий лист? (Виберіть декілька варіантів)

- Отримати віддалений доступ
- Паралізувати роботу комп'ютера за допомогою шифрування системи з метою вимагання грошей для відновлення файлів
- Зібрати секретні дані для входу у ваш обліковий запис
- Показати рекламу

9. Чому двофакторна система автентифікації дає додатковий рівень безпеки?

- Зловмисник не дізнається ваш пароль
- Коли є двофакторна автентифікація, вас неможливо знайти в Інтернеті
- Зловмисник не має доступу до приладу, який генерує секретні коди. Знаючи пароль, він не зможе увійти до вашого облікового запису, адже йому потрібно буде дізнатися секретний код, який змінюється на вашому телефоні кожні 30 секунд
- Дає більше часу, щоб встигнути змінити пароль

10. Чому пошта є настільки привабливою для злочинців? (Виберіть декілька варіантів)

- Поштовий сервіс безкоштовний
- Злочинці користуються людською психологією, щоб збільшити шанси відкриття шкідливих файлів (наприклад, маскуючись під…)
- Функція додатків до листів дає злочинцям змогу надсилати файли зі шкідливим програмним кодом
- Бази даних поштових скриньок легко знайти в мережі Інтернет

11. Який із наведених нижче файлів, надісланий як додаток до електронного листа, наймовірніше є ШПЗ?

- Звіт_жовтень_2020.doc
- Звіт_жовтень_2020.docx
- Звіт_жовтень_2020.doc.exe
- Звіт_жовтень_2020.pdf

12. Виберіть правильні твердження, що стосуються двофакторної автентифікації. (Виберіть декілька варіантів)

- Двофакторна автентифікація – це те саме, що двоетапна перевірка
- Суть двофакторної автентифікації полягає у двох способах підтвердження своєї особи для отримання доступу до інформації

- Якщо хакер знає ваш пароль, але не знає тимчасового коду, він все одно зможе зламати вашу сторінку
- Ключовим елементом захисту є тимчасовий код, який генерує певна програма/фізичний токен
- Усе вищеперераховане

Матеріал для опрацювання

Хто володіє інформацією,
той володіє світом.
Вінстон Черчилль

1. Онлайн-середовище та безпека. Кібергігієна

Чому розбиратися в основах інформаційної безпеки потрібно кожному, як навчати здобувачів освіти кіберграмотності та що робити, якщо учень хоче рятувати світ від комп'ютерних загроз?

У липні 2020 року хакери зламали безліч акаунтів у Twitter, включаючи верифіковані. Повідомлення про безкоштовну роздачу біткоїнів було опубліковано, зокрема, на сторінках Ілона Маска, Білла Гейтса, Барака Обами та деяких інших відомих людей. За допомогою цих публікацій зловмисники закликали користувачів переказувати свої кошти на певний гаманець та обіцяли подвоювати усі вхідні платежі. В результаті люди перевели щонайменше $120 тис. на вказаний у постах рахунок. Після інциденту представники Twitter підтвердили, що кібератака пішла за компрометацією одразу кількох співробітників компанії. Примітно, що шахраї організували атаку фішингу, застосувавши таким чином соціальну інженерію проти співробітників Twitter.

Те, що зловмисникам вдалося реалізувати таку масштабну кібератаку, ще раз доводить: методи соціальної інженерії залишаються одними з найдієвіших. Саме тому в сучасному світі володіння базовими правилами інформаційної безпеки так само потрібне, як, наприклад, знання основ здорового способу життя або пожежної безпеки. Причому формувати навички так званої кібергігієни у людей потрібно з ранніх років. Батькам слід розповідати своїм дітям про правила безпечної поведінки в інтернеті, як тільки юні користувачі отримують доступ до комп'ютера чи смартфона, подібно до того, як дитина дізнається про правила безпечного переміщення містом, коли вона починає самостійно ходити до закладу освіти.

Сучасні заклади освіти широко використовують цифрові технології у своїй діяльності для ведення журналів, контролю навчальних досягнень, адміністративної діяльності тощо. До проблем інформаційної безпеки відносять такі фактори: використання застарілих і свідомо небезпечних платформ; встановлення піратського програмного забезпечення; низька кваліфікація обслуговуючого персоналу, в ряді випадків відсутність посади фахівця з підтримки інформаційних систем; відсутність практики регулярного аудиту безпеки.

Для освітнього середовища проблема інформаційної безпеки пов'язана із захистом персональних даних абітурієнтів, здобувачів освіти, співробітників, включаючи їх особисту, фінансову, навчально-професійну та іншу інформацію. Таким чином, забезпечення інформаційної безпеки пов'язане з роботою всіх структурних підрозділів освітньої організації, починаючи з роботи приймальної комісії, навчальної частини і закінчуючи кадровою службою.

Сучасна людина є своєрідним заручником високих технологій. Важко відволікти увагу дитини від смартфону чи монітора комп'ютера? Діти повсякчас щось шукають в мережі чи завантажують з неї, спілкуються у чатах. Це може свідчити про інтернет-залежність. Як цьому запобігти?

Інтернет-залежність (або інтернет-адикція) — нав'язливе й неконтрольоване бажання людини підключатися до мережі інтернет і нездатність свідомо відключитися, вийти з мережі.

Інтернет сам по собі не є хорошим чи поганим – це просто частина світу, який нас оточує, – багато в чому корисна і потрібна. Будучи невичерпним джерелом інформації, інтернет приваблює дітей можливістю дізнатися і побачити все що завгодно. Цікава до всього дитина прагне отримати якомога більше: спілкування, ігор, мультфільмів, розваг – і тому багато часу проводить у віртуальному просторі, часто на противагу реальному життю. Соціалізацію і спілкування з однолітками замінює фактично однобоким онлайн-спілкуванням. Активним іграм на свіжому повітрі все більше дітей протиставлять мережеві ігри, далеко не завжди нешкідливі. Іноді пошук нової інформації стає буквально нав'язливою ідеєю.

Як виявити залежність?

Якщо у дитини спостерігаються деякі з перелічених нижче ознак, варто бити тривогу:

• збільшення інтервалу часу, проведеного з комп’ютером;

• зниження успішності;

• втрата інтересу до того, що відбувається навколо;

• втрата інтересу до позааудиторних занять;

• порушення сну;

• часті та різкі перепади настрою;

• неадекватна поведінка у відповідь на пропозицію вимкнути комп’ютер – аж до прояву агресії та сварки.

Інтернет може бути чудовим та корисним засобом для навчання, відпочинку чи спілкування з друзями. Але – як і реальний світ – Мережа також може бути небезпечною: у ній з’явилися своя злочинність, хуліганство та інші малоприємні речі. Віртуальність спілкування надає людям з недобрими намірами додаткові можливості заподіяти шкоду дітям. В останній час в Інтернеті з'являється багато матеріалів агресивного та соціально небезпечного змісту.

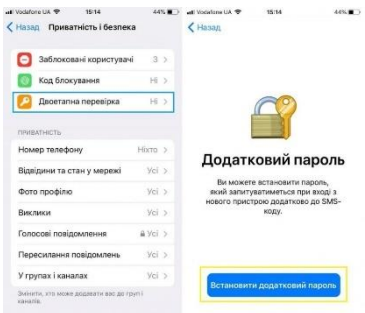
Дорослим слід пам'ятати про існування подібних загроз і приділяти особливу увагу питанню забезпечення безпеки здобувачів освіти в Інтернеті.

З кожним днем інформаційні технології все більше проникають в життя сучасної людини. Сьогодні майже кожен має смартфон з доступом до Інтернет-мережі, що дозволяє користувачам завжди бути онлайн. Зокрема у будь-яку мить ви можете перевірити пошту чи месенджер, купити квиток в кіно чи забронювати житло для відпустки та навіть здійснювати платежі, не звертаючись до відділень банку. Всі ці дії в Інтернеті передбачають обмін певною особистою інформацією чи конфіденційними даними, які у разі вашої неуважності можуть опинитися в руках зловмисників.

Для забезпечення захисту ваших персональних даних під час роботи в Інтернет-мережі спеціалісти рекомендують дотримуватися основних правил кібергігієни. В свою чергу кібергігієна — це заходи безпеки, розроблені для захисту пристроїв користувача від інфікування шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації.

Правила кібергігієни: 7 кроків для покращення захисту даних

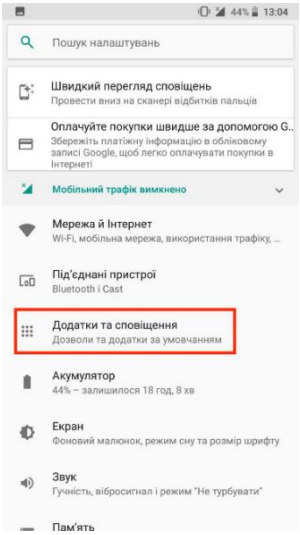
1. Перевірка безпеки активних акаунтів.



Першим правилом кібергігієни є перевірка безпеки вже існуючих облікових записів електронної пошти та акаунтів в соцмережах. Зокрема такі веб-сайти як haveibeenpwned.com та

breachalarm.com допоможуть з’ясувати, чи був пароль до електронної пошти викрадений зловмисниками.

2. *Аналіз програм.*

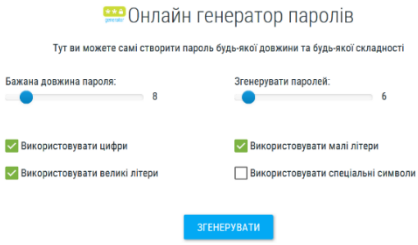


Сьогодні у кожного сайту, магазину та навіть банку є спеціальний мобільний додаток. Проте це не означає, що всі вони мають бути на вашому пристрої. Завантажуйте тільки необхідні для роботи програми. Спеціалісти радять проаналізувати вже завантажені додатки, видалити непотрібні та в подальшому ко нтролювати встановлення кожної програми. Також під час завантаження кожного додатку варто звертати увагу на дозволи, які ви надаєте. Часто шкідливі програми надсилають запит на отримання великої кількості дозволів, які не відповідають їх функціоналу. Це дозволяє збирати багато інформації про користувача з метою отримання прибутку.

3. *Регулярне оновлення.*

Для запобігання інфікуванню шкідливими програмами варто здійснювати своєчасне оновлення операційної системи та окремих додатків, яке передбачає виправлення уразливостей та помилок в програмному забезпеченні.

4. *Надійний пароль.*



З метою запобігання несанкціонованому доступу до пристроїв переконайтеся у надійності ваших паролів. Важливо створити складну комбінацію, яка містить не менше 12 символів, великі та малі літери, цифри та символи. Крім цього, для кожного акаунта варто використовувати унікальний пароль. Таким чином викрадення однієї з комбінацій не поставить під загрозу інші облікові записи. Більше рекомендацій за посиланням.

5. *Додатковий рівень захисту.*

Для покращення безпеки облікових записів використовуйте двофакторну аутентифікацію, яка передбачає підтвердження особистості під час входу в певний акаунт. Найчастіше для цього використовуються SMS-повідомлення або окрема програма. Таким чином у разі викрадення пароля зловмисники не зможуть отримати доступ до ваших даних.

6. *Регулярне резервне копіювання.*

Необхідним кроком для уникнення втрати важливих даних є регулярне резервне копіювання інформації на зовнішній жорсткий диск або у хмару. Це допоможе відновити потрібні дані у разі їх шифрування програмою-вимагачем або видалення шкідливим програмним забезпеченням.

7. *Надійний захист.*

Останнім, але не менш важливим, правилом кібергігієни є використання надійного рішення для захисту вашого комп'ютера чи смартфона від різних загроз, зокрема програм-вимагачів, шпигунських програм, вірусів, троянів та фішинг-атак.

Ці сім основних правил кібергігієни допоможуть вам своєчасно виявити підозрілу діяльність зловмисників та запобігти втраті персональних даних та іншої особистої інформації.

Запровадження дистанційного навчання на початку пандемії спонукало педагогічних працівників швидко шукати способи, інструменти та електронні канали комунікації для його проведення і взаємодії з учнями та батьками.

Цифровізація освітнього процесу й робота з технологіями дистанційного навчання вже помітно вплинула на те, як відбувається освітній процес.

З одного боку значно розширилися і продовжують розширюватися можливості педагогів проводити навчання, а учнів – навчатися.

З іншого – використання цих методів, технологій та інструментів тісно пов’язане з безпекою роботи, зокрема, використанням та обробкою персональних даних учасників освітнього процесу.

Існує певна проблема, пов'язана з засвоєнням основ інформаційної безпеки. Ніщо так не вчить фінансової грамотності, як втрата грошей, і ніщо так не вчить кіберграмотності, як витік персональних даних, зламування акаунту і знову ж таки втрата грошей. Або набагато більшого. Виникає закономірне питання про те, чи може людина, у тому числі дитина, навчитися дотримуватись правил особистої кібергігієни, уникнувши такого «суворого» досвіду. Може. Для цього необхідно подолати деякі негативні установки.

2. Документи, що регламентують роботу закладу освіти з персональними даними під час дистанційного навчання

Інформація з сайту - ОСВІТНІЙ ОМБУДСМЕН

В Україні поки ще немає чітко визначеної нормативної бази, яка б регулювала безпеку роботи викладачів та учнів в Інтернеті під час дистанційного навчання, у тому числі, – безпеку роботи з персональними даними. Але ніщо не заважає нам використовувати на практиці ті норми законодавства, які ми вже маємо.

Положення про дистанційну форму здобуття повної загальної середньої освіти визначає, що під час дистанційного навчання освітній процес організовується з дотриманням вимог законодавства про захист персональних даних (частина 9 Положення).

А у листі МОН № 1/9-609 від 02.11.20 року “Щодо організації дистанційного навчання” наголошується, що всі учасники освітнього процесу мають дотримуватися вимог щодо захисту персональних даних учасників освітнього процесу в електронному освітньому середовищі.

Основним законом із питання захисту персональних даних в нашій державі є Закон України “Про захист персональних даних”, і саме його потрібно брати за основу для роботи з персональними даними та їхнього захисту.

3. Дії закладу освіти задля безпеки дистанційного навчання

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. Під час дистанційного навчання викладачі та учні використовують особисті домашні пристрої, які зазвичай не охоплюються мережевим захистом. У такому випадку викладачам

та батькам учнів варто перевірити офіційність та надійність свого інтернет-провайдера, щоб оцінити можливі ризики. Якщо провайдер неофіційний – посилити захист за допомогою програмного забезпечення. Також ключове значення мають проведення для учнів навчання про безпеку в інтернеті, обговорення різних практичних випадків та діалог;

– використовувати програмне забезпечення для фільтрації та моніторингу безпеки пристроїв;

– встановлювати політику в межах закладу освіти, що регулює, де і як можуть використовувати технології різні учасники навчального процесу, а також порядок реагування на інциденти, пов'язані з безпекою дітей, зокрема, в цифровому середовищі;

– організовувати для здобувачів освіти навчання з питань онлайнової безпеки;

– забезпечувати достатній рівень підготовки усіх співробітників (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 онлайновою безпекою, щоб сформувати цілісне уявлення про наявні у школі проблеми та тенденції, що вимагають уваги;

– вжити заходів для того, щоб адміністративно-управлінський персонал та керівники були достатньо обізнані в питаннях онлайнової безпеки у закладі освіти;

– взяти до уваги потенційний вплив Інтернету та онлайнових технологій на навчання та психіку здобувачів освіти.

– Відповідно до Положення про дистанційну форму здобуття повної загальної середньої освіти, електронні освітні платформи, онлайн сервіси та інструменти, за допомогою яких організовується освітній процес під час дистанційного навчання, обирає та схвалює педагогічна рада закладу освіти (частина 5, розділ I Положення).

МОН наголошує на тому, що рекомендовано педагогам обирати для дистанційного навчання одну або дві освітні платформи, оскільки це полегшить учням, викладачам та батькам організацію навчання. Також використання мінімальної можливої для забезпечення освітнього процесу кількості платформ робить дистанційне навчання безпечнішим, оскільки зменшується ризик витоку персональних даних. Як у випадку з провайдером, рекомендуємо обирати перевірені платформи від офіційних виробників та не надавати зайвих персональних даних здобувачів освіти і викладачів для користування платформами. Заклад освіти має повідомити учнів та батьків, які персональні дані будуть оброблятися під час використання тієї чи іншої платформи дистанційного навчання.

Водночас закладам освіти необхідно звернути увагу на розробку певних правил поведінки та безпеки в онлайн середовищі і порядок реагування на інциденти. Спільне обговорення та прийняття цих правил з усіма учасниками освітнього процесу дозволить

мінімізувати неприємні випадки, які періодично трапляються під час дистанційного навчання.

4. Рекомендації педагогічним працівникам для безпеки дистанційного навчання

Міжнародний союз електрозв'язку визначає такі рекомендації для викладачів.

Насамперед необхідно слідкувати за безпекою та надійністю як домашніх так і робочих пристроїв, які ви використовуєте для проведення дистанційного навчання. Для цього:

– переконайтеся в тому, що всі пристрої надійно захищені та на них встановлено пароль. Учителі настільки ж вразливі перед кібератаками, шкідливими програмами, вірусами та зламами, як і всі інші. Важливо, щоб усі пристрої, які ви використовуєте, захищалися надійним паролем. Онлайн-генератор надійних паролів – сервіс 2ip.ua (https://2ip.ua/ua/services/useful-service/password-generator)

– блокуйте пристрої, завершуйте сеанс і виходьте з облікового запису, коли не використовуєте їх (наприклад, якщо виходите з кімнати або класу);

– встановіть антивірусне програмне забезпечення та брандмауер й регулярно їх оновлюйте.

Також дотримуйтеся визначеної закладом освіти політики щодо використання мобільних технологій та інших електронних пристроїв. Важливо, щоб при використанні пристроїв ви подавали учням приклад правильної поведінки.

Забезпечте фільтрацію та моніторинг даних, що передаються через шкільне під'єднання до Інтернету (під час дистанційного навчання вдома – через домашнє під'єднання до Інтернету). Здобувачі освіти не повинні отримувати доступу до шкідливого або неприйнятного контенту через ІТ-системи закладу освіти або домашнє технічне обладнання. Системи фільтрації мають щонайменше блокувати доступ до незаконного контенту, а також контенту, який вважається неприйнятним або шкідливим.

Необхідно пам'ятати про власну онлайн-репутацію та цифровий слід, який залишаєте, про те, що ваші слова та дії в Інтернеті можуть вплинути як на вашу власну репутацію, так і на репутацію закладу освіти. Також розповідайте дітям про важливість онлайнової репутації й про те, як правильно її формувати.

Між приватним та професійним життям педагогів завжди має бути чітка межа, зокрема, й у цифровому середовищі. Для будь-яких контактів між співробітниками закладу освіти та здобувачами освіти або батьками завжди необхідно використовувати

корпоративну електронну пошту. Комунікаційна політика закладу освіти може забороняти будь-які контакти, не пов'язані з освітньою діяльністю, та контакти на платформах, що не мають стосунку до закладу освіти.

На випадок проведення відеоконференцій або занять у віддаленому режимі, заклади освіти мають установлювати чіткі приписи як для співробітників, так і для учнів (наприклад, що бажано підготувати місце для віддаленого заняття/сеансу зв'язку та подбати про тих, хто перебуває поруч – чи то вдома, чи то в класі).

Викладачі мають розуміти, чим Інтернет може бути для учнів небезпечний і чим корисний. З рекомендаціями щодо захисту дітей в мережі інтернет можна докладно ознайомиться у Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі, розробленими Міжнародним союзом електрозв'язку (МСЕ) та робочою групою авторів із провідних установ, що працюють у індустрії інформаційно-комунікаційних технологій (ІКТ) і переймаються проблемами захисту дитини (в цифровому середовищі), зокрема за посиланням https://thedigital.gov.ua/storage/uploads/files/news_post/2021/1/za-initsiativi-mintsifri-pidgotuvali-rekomendatsii-shchodo-zakhistu-ditey-u-tsifrovomu-seredovishchi/COP-Guidelines-for-Parents-Educators-UAfin.pdf

Для безпеки педагогів експерти радять створити окремий обліковий запис або окремого користувача, якщо ділите вдома чи на роботі свій пристрій ще з кимось, і також розмежувати ваші власні електронні скриньки для особистого користування та для робочих питань.

Необхідно також звертати особливу увагу на пересилання персональної інформації (власної або здобувача освіти) через соціальні мережі, різноманітні месенджери, електронною поштою. Поміркуйте, чи дійсно необхідно надсилати персональні дані у повідомленні. Якщо це все ж необхідно, потрібно ретельно перевірите, чи правильно вказана адреса адресата.

5. Рекомендації для батьків

Захист персональних даних – це спільна робота педагогів, батьків та учнів. Тому чималу роль у тому, чи буде дистанційне навчання успішним, якісним та безпечним для дитини, відіграють батьки. Просимо вас розповісти дітям про персональні дані, про небезпеку їхнього поширення і правила поводження з ними.

Для батьків Міжнародний союз електрозв'язку визначає такі рекомендації.

1. Насамперед спілкуйтеся зі своїми дітьми, цікавтеся, що вони люблять переглядати в Інтернеті, спробуйте організувати спільно з ними будь-яку онлайнову діяльність.

2. Визначте, які технології, пристрої та послуги використовуються у вас вдома.

3. Встановіть на всіх пристроях брандмауер та антивірусну програму. Поміркуйте над тим, чи будуть корисними та чи підходять для вашої родини програми фільтрації, блокування або відстеження. Розгляньте можливість використання контент-фільтрів, що досить часто називаються системами батьківського контролю, і безпечних пошукових систем або обмежень доступу, щоб фільтрувати контент, який діти можуть переглядати в Інтернеті.

4. У колі родини домовтеся про умови використання Інтернету й особистих пристроїв, приділяючи особливу увагу питанням конфіденційності, вікової відповідності змісту сайтів, додатків та ігор, булінгу, кількості проведеного перед екраном часу та небезпеки з боку незнайомців.

5. Поясніть дітям, що перш ніж публікувати світлини або відео в Мережі, слід отримати згоду людей, які там зображені. Батькам також варто звертати увагу на те, якою інформацією про своїх дітей вони діляться в соціальних мережах і в Інтернеті загалом, зокрема, це стосується особистих історій про дітей або їхніх світлин. Пам’ятайте про недоторканність приватного життя вашої дитини!

6. Поясніть дітям, що не можна повідомляти свої паролі доступу друзям або братам і сестрам. Звертайте їхню увагу на те, коли і де вони повідомляють свою персональну інформацію – наприклад, навчайте, що в загальнодоступному профілі краще використовувати деперсоніфіковані зображення як фотографії профілю і вказувати мінімум персональної інформації, такої як вік, школа та місце проживання.

7. Зверніть увагу на вік «цифрової згоди». У деяких країнах діють закони, що встановлюють мінімальний вік, починаючи з якого компанії або вебсайти можуть просити дітей повідомити персональну інформацію без попереднього отримання підтвердженої згоди батьків. Вік «цифрової згоди» зазвичай варіюється в межах 13-16 років. На багатьох вебсайтах, призначених для дітей молодшого віку, потрібна згода батьків для реєстрації нового користувача.

8. Дізнайтеся, як повідомити про проблему на платформах, якими користуються ваші діти, і як видалити профіль або змінити зазначену в ньому інформацію.

9. Розкажіть про важливість персональної інформації. Поясніть дітям, що їм слід ділитися тільки тією інформацією, яку, на вашу і на їхню думку, дозволено побачити стороннім. Їм не слід ділитися інформацією, що дозволяє встановити їхню особистість або

особистість інших. Нагадайте дітям, що в них є онлайн репутація, за якою необхідно стежити, а після того, як контент опубліковано, його може бути складно змінити або скорегувати.

10. Переконайтеся, що діти розуміють, що означає публікація світлин та відео в Інтернеті, в тому числі їхніх власних та їхніх друзів. Поясніть дітям, що фотографії та відео можуть розкривати безліч персональної інформації. Діти повинні розуміти ризики, пов'язані з використанням камер та опублікуванням контенту. Бажано, щоб світлини інших людей не викладалися без їхньої згоди. Це також стосується і батьків, які роблять та публікують знімки своїх дітей. Крім того, важливо, щоб діти розуміли, що іноді інформацію може розкрити хтось із їхніх друзів або членів сім'ї, тому їм варто поговорити про це зі своїми друзями та родичами і розповісти про небезпеку надмірного розкриття інформації. Порадьте своїм дітям не викладати власні фото та відео або фото та відео друзів, на яких є елементи, що легко піддаються ідентифікації, наприклад, таблички з назвами вулиць, автомобільні номери або назва заклади освіти на толстовках тощо.

Всі учасники освітнього процесу повинні з повагою ставтеся один до одного, адже безпека як очного, так і дистанційного навчання залежить від педагогів, батьків, здобувачів освіти.

6. Правила інформаційної війни: як не нашкодити і бути корисним в Інтернеті

Національна гвардія України закликала громадян, які не можуть допомагати на полі бою чи займатися волонтерством, вступати у боротьбу з ворогом в інформаційній війні. Для цього необхідно дотримуватись кілька правил інформаційному фронті:

Правило 1

Інформація, котру ви поширюєте у мережах і серед знайомих повинна бути корисною. ***Корисна інформація*** виконує завдання, котрі пришвидшують нашу перемогу. Вона може підіймати бойовий дух наших воїнів, волонтерів і працівників галузей критичної промисловості. Вона може демотивувати ворога. Може підтримувати вимушених переселенців. Корисна інформація повинна мати ціль, а перед поширенням будь-якої інформації варто задати собі питання: а який ефект вона має спричинити? Якщо ви розумієте користь – тоді поширюйте.

Правило 2

Якщо ви хочете бути максимально корисними на інформаційному фронті, ***то не варто продукувати і ділитися великою кількістю матеріалів, котрі мають різні (часом***

протилежні) меседжі. Найкращий ефект буде тоді, коли ви методично і постійно будете популяризувати одну або кілька позицій, думок чи закликів. Наприклад, українці зі всього світу допомогли українським дипломатам добитися відключення Росії від системи SWIFT, тому що на порядку денному це питання було найпомітніше і про нього говорили і політики, і журналісти, і громадський сектор і звичайні громадяни. Якщо спільно тиснути в одну точку – це прискорить прогрес.

Правило 3

Будьте обережні з неперевіреною інформацією і фейками. Нам може здаватися, що якщо фейк пришвидшить нашу перемогу, то це корисний фейк, проте тут є певний підступ. Річ у тім, що ейфорія спричинена фейком дуже швидко може переростати у розчарування і недовіру. А недовіра - дуже добрий ґрунт для ворожої пропаганди. Важливу чи підозрілу інформацію краще перевіряти на офіційних сторінках командування і у якісних медіа.

Правило 4

На інформаційному фронті краще боротися групами. Зараз є безліч ініціатив, котрі працюють як на українську аудиторію, так і для людей за кордоном. Хтось через комунікацію з медіа, хтось через спілкування з іноземцями на пряму, хтось записує відео різними мовами, а хтось перекладає матеріали і збирає докази російських військових злочинів. Кожен може знайти собі застосування. Для пошуку найвідповіднішого для вас завдання використовуйте гештеґи. Це допоможе організуватися і знайти однодумців.

Правило 5

Не нашкодь. До інформації потрібно ставитися відповідально. Наші військові не раз просили не вести прямі трансляції обстрілів, бо це може допомогти ворогу у коригуванні вогню. Також пам’ятайте, що ваші фото мають зашиті в собі геолокацію, тому дуже обережно фотографуйте і діліться світлинами, котрі зроблені поруч з позиціями українських військових чи стратегічними об’єктами.

САМОСТІЙНА РОБОТА

Тема 3. Удосконалення рівня цифрової компетентності учасників освітнього процесу з кібербезпеки: інструменти, технології (2 год.)

Питання до самостійного заняття

1. Закон ЄС про кібербезпеку (Cybersecurity Act).

2. Перший законодавчий акт Європейського Союзу з кібербезпеки – Директива Європейського Союзу в сфері мережевої та інформаційної безпеки (NIS) Сутність та визначення понять «інформаційна безпека» та «безпека інформації».

3. Ключові принципи захисту персональних даних у європейському законодавстві.

4. Основна спрямованість національного законодавства у сфері забезпечення захисту інформації.

Завдання

Ознайомтеся із середовищем дистанційної освіти Cisco NetAcad міжнародної мережевої академії Cisco (https://id.cisco.com/).

Проблемно-пошукові питання до самостійної роботи

1. Поміркуйте, за якими принципами мають розвиватися взаємовідносини між Україною та НАТО у сфері інформаційної та кібернетичної безпеки? Назвіть основні напрямки співробітництва Україна–НАТО у сфері кіберзахисту
2. Поміркуйте над поняттям «кібертероризм». Наведіть приклади його тлумачення різними категоріями дослідників.
3. Перелічіть основні кроки, які мають бути дотримані співробітниками служб безпеки в разі фіксації порушень інформаційної та кібернетичної безпеки.
4. Що слід розуміти під поняттям інциденту у сфері високих технологій? Розкрийте сутність процесу управління інцидентами. Як класифікує інциденти у сфері високих технологій Рада Європи? Який зміст у це поняття вкладають такі провідні країни світу, як США, Німеччина, Франція, Великобританія?

КОМПЛЕКС ПРАКТИЧНИХ (ТЕСТОВИХ) ЗАВДАНЬ ДЛЯ САМОКОНТРОЛЮ

До теми 1. Поняття кібербезпеки. Он-лайн та оф-лайн ідентифікація. Методи та засоби захисту конфіденційної інформації, персональних даних учасників освітнього процесу

1. Кібербезпека –

а) це безпека IT систем (обладнання та програм)

б) збереження конфіденційності, цілісності та доступності інформації

в) це базовий комплекс програм, що виконує керування апаратною складовою комп'ютера

2. З який трьох основних ланок складається безпека?

а) конфіденційність, цілісність та доступність

б) програмне забезпечення, апаратне забезпечення та комунікації

в) люди, технології, процеси

3. На які три частини можна розділити Інформаційні системи?

а) конфіденційність, цілісність та доступність

б) програмне забезпечення, апаратне забезпечення та комунікації

в) люди, технології, процеси

4. Які три елементи є складовими тріади CAI? (Виберіть три варіанти.)

а) доступність (availability)

б) доступ (access)

в) втручання (intervention)

г) масштабованість (scalability)

д) конфіденційність (confidentiality)

є) цілісність (integrity)

5. Який метод використовується для перевірки цілісності даних?

а) шифрування (encryption)

б) аутентифікація (authentication)

в) резервне копіювання (backup)

г) контрольна сума (checksum)

6. Які три методи можуть бути використані для забезпечення конфіденційності інформації? (Оберіть три варіанти.)

а) контроль версій (version control)

б) резервне копіювання (backup)

в) двофакторна аутентифікація (two factor authentication)

г) налаштування прав доступу для файлів (file permission settings)

д) шифрування даних (data encryption)

є) логін та пароль (username ID and password)

7. Як ще називають конфіденційність інформації?

а) точність (accuracy)

б) узгодженість (consistency)

в) приватність (privacy)

г) достовірність (trustworthiness)

8. У чому причина того, що внутрішні загрози безпеці можуть заподіяти більшу шкоду для організації, аніж зовнішні загрози?

а) Внутрішні користувачі мають кращі навички хакерства.

б) Внутрішні користувачі мають прямий доступ до пристроїв інфраструктури.

в) Внутрішні користувачі можуть отримати доступ до пристроїв інфраструктури через Інтернет.

г) Внутрішні користувачі можуть отримати доступ до корпоративних даних без аутентифікації.

9. Що таке "Браузер"?

а) програма, призначена для захисту операційної системи від вірусів

б) це програма, яка дозволяє відображати веб-сторінки

в) базовий комплекс програм, що виконує керування апаратною складовою комп'ютера

10. Що таке "https://"?

а) небезпечне з'єднання без замочка

б) безпечне з'єднання, позначене замочком

в) набір правил передачі файлів (тексту, зображень, відео) через Інтернет

11. Домен -

а) дозволяє відображати веб-сторінки

б) це адреса веб ресурсу в мережі інтернет

в) місце куди ми вводимо доменне ім'я сайту

12. Співставте типи кіберзлочинців з їхнім описом

Роблять політичні заяви або залякують, завдаючи жертвам фізичної або психологічної шкоди	Терористи
Від імені уряду збирають інформацію або здійснюють саботаж, спрямований на конкретні цілі	Нападники, що спонсоруються державою
Роблять політичні заяви для формування обізнаності з важливих для них питань	Хактивісти

До теми 2. Забезпечення інформаційної безпеки учасників освітнього процесу в ЗП(ПТ)О

1. Користувач працює в Інтернеті, використовуючи ноутбук та загальнодоступний WiFi у кафе. Що слід перевірити перш ніж підключитися до загальнодоступної мережі?

а) чи встановлено на ноутбуці майстер-пароль для захисту паролів, що зберігаються у менеджері паролів

б) чи відімкнено адаптер Bluetooth на ноутбуці

в) чи ноутбук вимагає автентифікації користувача для спільного використання файлів і медіа

г) чи веб-браузер ноутбука працює у приватному режимі

2. Як можуть користувачі, що працюють на комп'ютері, відкритому для спільного використання, приховати історію своїх веб-переглядів від інших працівників, які також можуть використовувати цей комп'ютер?

а) Перемістити завантажені файли у кошик.

б) Використовувати веб-браузер у режимі приватного (анонімного) перегляду.

в) Перезавантажити комп'ютер після закриття веб-браузера.

г) Для доступу до веб-сайтів використовувати лише зашифроване з'єднання.

3. Антивірус це

а) базовий комплекс програм, що виконує керування апаратною складовою комп'ютера

б) шифрує всі файли, а потім вимагає викуп за розшифровку

в) це спеціалізована програма, призначена для захисту операційної системи від вірусів

4. Який найпоширеніший метод виманювання конфіденційної інформації?

а) Фішинг

б) Спам

в) Вішинг

5. Що таке "Дорожнє яблуко"?

а) метод соціальної інженерії, що поєднує в собі ознаки фішингу та вішингу

б) різновид фішингу, який здійснюється через телефон

в) метод атаки, який передбачає підкинути співробітнику компанії чи установи фізичний

г) носій інформації (флешку) зі шкідливим програмним забезпеченням

6. Який найпоширеніший метод виманювання конфіденційної інформації?

а) Фішинг

б) Спам

в) Вішинг

7. Яка має бути мінімальна довжина паролю?

а) не менше 8 символів

б) не менше 4 символів

в) не менше 6 символів

8. Кілогер

а) шифрує всі файли, а потім вимагає викуп за розшифровку

б) використовує потужність вашого ПК чи телефону з метою видобутку криптовалюти

в) перехоплює інформацію з натиснутих клавіш на клавіатурі, кліки миші, робить знімки екрану, перехоплює дані з веб камери та принтера

9. Вішинг це

а) різновид фішингу, який здійснюється через телефон

б) різновид фішингу, який здійснюється через соцмережі

в) різновид фішингу, який здійснюється через елекронну пошту

10. Хто найслабший у системі безпеки?

а) технології

б) процеси

в) люди

11. Протокол це

а) небезпечне з'єднання

б) безпечне з'єднання

в) набір правил передачі файлів (тексту, зображень, відео) через Інтернет

12. Соціальна інженерія -

а) це мистецтво маніпулювання людьми через виконання дій, або розголошення конфіденційної інформації

б) різновид фішингу, який здійснюється через SMS розсилки

в) різновид фішингу, який здійснюється через телефон

До теми 3. Удосконалення рівня цифрової компетентності учасників освітнього процесу з кібербезпеки: інструменти, технології

1. Троянська програма -

а) головною метою є розмноження серед комп'ютерів у мережі

б) надає віддалений доступ до комп'ютера для зловмисників

в) програма, яку користувачі завантажують та запускають власноруч під виглядом корисних програм

2. Фішинг -

а) вид соціальної інженерії, за якої особа сама звертається до шахрая та повідомляє свої конфіденційні дані

б) це багаторівнева атака, в ході якої хакер атакує менш захищену проміжну організацію чи установу

в) найпоширеніший метод виманювання конфіденційної інформації

3. Кві про кво – це

а) метод соціальної інженерії, що поєднує в собі ознаки фішингу та вішингу

б) різновид фішингу, який здійснюється через телефон

в) найпоширеніший метод виманювання конфіденційної інформації

4. Зворотна соціальна інженерія -

а) метод атаки, який передбачає підкинути співробітнику компанії чи установи фізичний носій інформації (флешку) зі шкідливим програмним забезпеченням

б) метод соціальної інженерії, що поєднує в собі ознаки фішингу та вішингу

в) вид соціальної інженерії, за якої особа сама звертається до шахрая та повідомляє свої конфіденційні дані

5. Операційна система -

а) шифрує всі файли, а потім вимагає викуп за розшифровку

б) використовує потужність вашого ПК чи телефону з метою видобутку криптовалюти

в) базовий комплекс програм, що виконує керування апаратною складовою комп'ютера

6. Соціальна інженерія -

а) це мистецтво маніпулювання людьми через виконання дій, або розголошення конфіденційної інформації

б) різновид фішингу, який здійснюється через SMS розсилки

в) різновид фішингу, який здійснюється через телефон

7. Яка головна мета зловмисників?

а) електронна пошта

б) фінансові дані

в) номер телефону

8. Що робить "Бекдор"?

а) встановлює троянські програми

б) надає віддалений доступ до комп’ютера для зловмисників

в) розмножується у комп'ютерній мережі

9. Що таке "Двофакторна аутентифікація"?

а) це спосіб входу до акаунту, при якому потрібно крім введення логіну та паролю виконати додаткову дію

б) зберігає ваші облікові дані для входу та допоможе вам за допомогою функції автоматичного входу для різних веб-сайтів та програм

в) комплексна оцінка системи безпеки в режимі «онлайн»

10. Як ви користуєтесь онлайн-банкінгом?

а) лише з перевірених мереж і пристроїв

б) підключаюся до публічного Wi-Fi у ТРЦ

в) підключаюся до публічного Wi-Fi у кафе

11. Що таке "Адресний рядок"?

а) дозволяє відображати веб-сторінки

б) місце куди ми вводимо доменне ім'я сайту

в) це адреса веб ресурсу в мережі інтернет

12. Що таке "http://"?

а) безпечне з'єднання, позначене замочком

б) безпечне з'єднання, яке шифрується

в) небезпечне з'єднання

13. Користувач працює в Інтернеті, використовуючи ноутбук та загальнодоступний WiFi у кафе. Що слід перевірити перш ніж підключитися до загальнодоступної мережі?

а) чи встановлено на ноутбуці майстер-пароль для захисту паролів, що зберігаються у менеджері паролів

б) чи відімкнено адаптер Bluetooth на ноутбуці

в) чи ноутбук вимагає автентифікації користувача для спільного використання файлів і медіа

г) чи веб-браузер ноутбука працює у приватному режимі

14. Який тип технології може запобігти зловмисному програмному забезпеченню відстежувати дії користувачів, збирати особисту інформацію та створювати небажані оголошення, що з'являються на комп'ютері користувача?

а) менеджер паролів

б) антишпигунське ПЗ (antispyware)

в) фаєрвол (брандмауер)

г) двофакторна аутентифікація

15. При зберіганні інформації на локальному жорсткому диску який спосіб захистить дані від несанкціонованого доступу?

а) шифрування даних

б) створення копії жорсткого диска

в) двофакторна аутентифікація

г) видалення важливих файлів

16. Який найкращий спосіб запобігти несанкціонованому використанню вашого Bluetooth?

а) Використовуйте Bluetooth лише під час під'єднання до відомого SSID.

б) Використовуйте Bluetooth лише для підключення до смартфона або планшета.

в) Завжди використовуйте VPN під час з'єднання з Bluetooth.

г) Завжди відключайте Bluetooth, коли він активно не використовується.

17. Адміністратор мережі проводить тренінг для співробітників офісу про те, як створити надійний і ефективний пароль. Який пароль, найімовірніше, буде найважче вгадати або зламати злочинцеві?

а) 10characters

б) drninjaphd

в) mk$$cittykat104#

г) super3secret2password1

18. Яке налаштування на бездротовому маршрутизаторі вважається нестандартним з точки зору безпеки бездротової мережі?

а) застосування шифрування WPA2

б) заборона широкомовної трансляції SSID

в) зміна стандартного SSID та пароля бездротового маршрутизатора

г) активація бездротової безпеки

19. Як користувач може завадити іншим прослуховувати мережний трафік під час роботи ПК через загальнодоступну точку доступу Wi-Fi?

а) Використовувати шифрування WPA2.

б) Відключити Bluetooth.

в) Створити сильні та унікальні паролі.

г) З'єднуватися з використанням служби VPN.

20. Споживач хоче роздрукувати фотографії, що зберігаються на обліковому записі у хмарному сховищі використовуючи службу друку в Інтернеті третьої сторони. Після успішного входу в обліковий запис у хмарі клієнтові автоматично надають доступ до служби онлайн-друку третьої сторони. Що дозволило виконати цю автоматичну аутентифікацію?

а) Користувач перебуває у незашифрованій мережі і пароль служби хмарного зберігання доступний для перегляду службі онлайн-друку.

б) Пароль, введений користувачем для служби онлайн-друку, аналогічний паролю, який використовується в службі хмарного зберігання.

в) Служба хмарного зберігання є довіреним програмним забезпеченням для служби онлайн-друку.

г) Інформація про обліковий запис для служби хмарного зберігання була перехоплена шкідливою програмою.

21. Користувачеві важко запам'ятовувати паролі для декількох облікових записів у Інтернеті. Яке найкраще рішення варто спробувати користувачеві для вирішення цієї проблеми?

а) Записати паролі на папері й ретельно їх заховати.

б) Повідомити паролі адміністратору мережі або комп'ютерному спеціалісту.

в) Створити єдиний надійний пароль, який буде використовуватися для усіх облікових записів у Інтернеті.

г) Зберегти паролі в централізованій програмі менеджера паролів.

22. Яка технологія дозволяє користувачу уникнути витрат на обладнання та технічне обслуговування при створенні резервних копій даних?

а) магнітна стрічка

б) мережне сховище (network attached storage)

в) хмарний сервіс

г) зовнішній жорсткий диск

ГЛОСАРІЙ КЛЮЧОВИХ СЛІВ

Адресний рядок - місце куди ми вводимо доменне ім'я сайту.

Антивірус - це спеціалізована програма, призначена для захисту операційної системи від вірусів, шпигунських програм, хакерських атак та іншого несанкціонованого доступу з метою крадіжки цінних особистих даних, або несанкціонованого управління комп'ютером.

Багатофакторна автентифікація (БФА) додає ще один рівень захисту під час входу. Під час доступу до облікових записів або програм користувачі проходять додаткову перевірку ідентичності, наприклад сканують відбиток пальця чи вводять код із телефона

Безпечна інформаційна система – це система, яка, по-перше, захищає дані від несанкціонованого доступу, по-друге, завжди готова надати їх своїм користувачам, а по-третє, надійно зберігає інформацію і гарантує незмінність даних.

Браузер, Web browser – спеціальна програма, призначена для перегляду веб-сайтів

Брандмауер (Brandmauer) – комп'ютерна програма, метою якої є захист комп'ютера від вірусів і хакерських атак) для фільтрації зв'язку між комп'ютером та Інтернетом.

Ботнет – це мережа комп'ютерів, інфікована шкідливим програмним забезпеченням.

VPN або «віртуальна приватна мережа» – це сервіс, який захищає ваше інтернет-з'єднання і конфіденційність в Інтернеті.

Віруси вимагачі (Ransomware - англ. ransom — викуп і software — програмне забезпечення). Це шкідливе програмне забезпечення, яке блокує пристрій або шифрує його вміст, вимагаючи гроші у жертв.

Вішинг та смішинг — це методи соціальної інженерії, подібні до фішингу, але здійснюються не через електронну пошту. Зокрема, вішинг реалізовується через шахрайські телефонні дзвінки, а для смішингу використовуються текстові SMS-повідомлення, які містять шкідливі посилання або вміст.

Дезінформація – це неправдива, маніпулятивна або оманлива інформація, що цілеспрямовано розповсюджується для досягнення певної мети.

Зміст курсу

Додатки — це сторонні додатки та сервіси, які мають певний доступ до вашого облікового запису.

«Дорожнє яблуко» («road apple»), або «Троянський кінь», — це метод атаки, який передбачає підкинути співробітнику компанії чи установи фізичний носій інформації (флеш-накопичувач, диск) зі шкідливим програмним забезпеченням.

Домен – це адреса веб ресурсу в мережі інтернет.

Доступність (availability) – гарантія того, що авторизовані користувачі завжди будуть отримувати доступ до даних. Доступність говорить про те, що дані відкриті лише для тих, у кого є відповідні дозволи.

«Зворотна соціальна інженерія» — це вид соціальної інженерії, за якої особа сама звертається до шахрая та повідомляє свої конфіденційні дані.

Інформаційна безпека - збереження конфіденційності, цілісності та доступності інформації. **Кібербезпека** є частиною Інформаційної безпеки.

Кібератака – це спроба реалізації загрози. Тобто, це дії кіберзловмисників або шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу.

Кібербезпека – це сукупність технічних і соціальних засобів, стратегій, принципів для забезпечення захисту суспільства від загроз і впливів з небажаними наслідками, що походять від інтернет-середовища.

Кібервійна - це будь-який віртуальний конфлікт, розпочатий як політично мотивована атака на комп'ютерні та інформаційні системи противника.

Кібергігієна — це заходи безпеки, розроблені для захисту пристроїв користувача від інфікування шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації.

Кіберпростір — це та частина цифрового середовища, де і завдяки якій відбувається контроль та керування різними фізичними об’єктами, для чого використовуються як певне програмне забезпечення та протоколи комп’ютерних мереж (зокрема Інтернет), так і інфраструктура мереж та телекомунікаційні канали.

Конфіденційність (confidentiality) – гарантія того, що секретні дані будуть доступні тільки тим користувачам, яким цей доступ дозволений (такі користувачі називаються авторизованими).

Менеджер паролів - це програма, яка зберігає ваші облікові дані для входу та допоможе вам за допомогою функції автоматичного входу для різних веб-сайтів та програм.

Месенджер – це спеціальний додаток або програма, яку завантажують і встановлюють на смартфон або комп'ютер.

Міжмережний екран (фаєрвол, брандмаурер) – це стіна або перегородка, яка призначена для запобігання поширенню вогню з однієї частини будівлі в іншу.

Онлайн-ідентичність — це те, як ви представляєте себе іншим в Інтернеті.

Операційна система (ОС) — це базовий комплекс програм, що виконує керування апаратною складовою цифрового пристрою.

Офлайн-ідентичність – це ви самі, особа, з якою ваші друзі та сім'я взаємодіють щодня вдома або на роботі.

Пароль — таємне слово або певна послідовність символів, призначена для підтвердження особи або її прав.

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

Протокол - набір правил передачі файлів (тексту, зображень, відео) через Інтернет.

Складна атака через проміжну ціль («Supply chain attack») — це кількаступенева атака, в ході якої хакер атакує не напряму організацію, яка його цікавить, а менш захищену проміжну організацію чи установу, а вже через неї компрометує ту ціль, яка від самого початку його цікавила.

Соціальна інженерія – це мистецтво маніпулювання людьми через виконання дій, або розголошення конфіденційної інформації.

Спам — це масове розсилання небажаних листів. Найчастіше спам — це лист електронної пошти, який надсилається одразу на велику кількість адрес, але він також може бути доставлений через миттєві повідомлення, SMS та соціальні мережі.

Cookie – це невеликі текстові файли, які зберігаються в комп’ютері під час відвідування певних веб-сторінок

SMS-фішинг (**смішинг**)— різновид фішингу, який здійснюється через SMS-розсилки. Одним із яскравих прикладів є SMS-повідомлення нібито про виграш великої суми грошей або автомобіля.

Телефонне шахрайство – це вид шахрайства, коли шахрай телефонує і переконує жертву повідомити особисту, фінансову чи конфіденційну інформацію або переказати гроші.

Фейк (з англ. Fake — підробка) - свідомо перекручена або повністю вигадана новина. Одна з найпоширеніших форм маніпуляцій у медіа.

Фішинг (саме слово є омофоном англійського слова «Fishing» (рибалка), оскільки техніка використовує ту ж логіку «вилову») — це форма кібератаки, під час якої злочинець намагається завойовувати довіру до жертви для виманювання конфіденційної інформації.

Хмарні сервіси дають можливість працювати з документами в браузері, спільно редагувати і автоматично зберігають внесені зміни. Дозволяють синхронізувати будь-які файли між пристроями та автоматично створюють резервні копії.

Цілеспрямований фішинг — це форма фішингу, під час якої зловмисник надсилає повідомлення, спрямовані на конкретну групу людей, або навіть просто окрему особу з метою викрадення даних або маніпулювання ними в зловмисних цілях.

Цілісність (integrity) – гарантія збереження даними правильних значень, яка забезпечується забороною для неавторизованих користувачів будь-яким чином змінювати, модифікувати, руйнувати або створювати дані.

Шифрування — це процес перетворення інформації у форму, в якій неавторизована сторона не зможе її прочитати.

ЦИФРОВА БІБЛІОТЕКА

1. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.

2. Корченко, О. Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти / О. Г. Корченко, В. Л. Бурячок, С. О. Гнатюк // Безпека інформації.— 2013.— Т. 19, № 1.— с. 40–45

3. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.)

4. Про національну безпеку України: : за станом на 15.06.2022 р. / Закон України, затверджений ВР України 21.06.2018 р., № 2469-VIII [Електронний ресурс].— Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19#Text

5. Про основні засади забезпечення кібербезпеки України: За станом на 17.08.2022 / Закон України, затверджений ВР України 05.10.2017 р. № 2163-VIII [Електронний ресурс].— Режим доступу: http://zakon0.rada.gov.ua/laws/show/2163-19

6. Про захист персональних даних: за станом на 19.08.2022 / Закон України від 01.06.2010 р. № 2297-VI [Електронний ресурс].— Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text

7. Про Національну програму інформатизації: за станом на 01.01.2022 / Закон України від 04.02.1998 р. № 74/98-ВР [Електронний ресурс].— Режим доступу: http://zakon0.rada.gov.ua/laws/show/74/98-вр

8. Ігнатушко Ю.І. Правові засади регулювання забезпечення кібербезпеки в Україні VIII [Електронний ресурс].— Режим доступу: http://dspace.oduvs.edu.ua/bitstream/123456789/471/1/ilovepdf_com-18-19%5B1%5D.pdf

9. Організація комп'ютерних мереж [Електронний ресурс] : підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Електронні текстові дані (1 файл: 45,7 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с

10. Курс мережевої академії Cisco: Cybersecurity Essentials, 2020. Режим доступу: https://www.netacad.com/courses/cybersecurity/cybersecurity-essentials

11. 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-mintsifri-pidgotuvali-rekomendatsii-shchodo-zakhistu-ditey-u-tsifrovomu-seredovishchi/COP-Guidelines-for-Parents-Educators-UAfin.pdf