ПРОГРАМА
курсу за вибором (вибірковий модуль)

«Введення у кібербезпеку»

(Войцеховський М.О., Гапонюк Ю.М., Густяк О.М., Дзюба С.М., Проценко Т.Г.)

Київ – 2018

Пояснювальна записка

Розвиток суспільства у 21-му сторіччі не можна уявити без комп'ютерів, комп'ютерних мереж, Інтернету. У повсякденному спілкуванні слово Інтернет означає не лише глобальну мережу, яка об'єднує мільйони комп'ютерів і локальних мереж усього світу, а єдиний глобальний інформаційний простір – сукупність взаємопов'язаних інформаційних ресурсів, програмного забезпечення, баз та банків даних, що обробляються в комп'ютерних мережах. З появою цього феномена величезна кількість користувачів отримали можливість дуже швидко отримувати потрібну інформацію з найбільш трастових і компетентних джерел. Мільйони людей можуть блискавично здійснювати обмін інформацією, спілкуватися незалежно від того, в якому місці земної кулі вони знаходяться, переглядати книги і кінофільми, зберігати особисті фотоальбоми.

За короткий проміжок часу Інтернет значно змінив наш спосіб життя, включаючи робочі процеси, способи навчання і розваг. Останнім часом до Інтернету здійснюється підключення не тільки комп'ютерів, а й всіляких фізичних пристроїв – «речей», оснащених сенсорами, датчиками і пристроями передачі інформації, які людина може використовувати в повсякденному житті, наприклад, холодильників, кондиціонерів, автомобілів, велосипедів і навіть кросівки.

Усі види організацій та установ нині використовують цю мережу для ефективного функціонування, зокрема для збору, обробки, обміну та зберігання великої кількості цифрової інформації.

Проте поряд з перевагами сучасного цифрового світу і розвитком інформаційних технологій, в цей час активно поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення персональних даних, незаконних фінансових операцій, крадіжок і шахрайства в мережі Інтернет. Сучасні інформаційно-комунікаційні технології використовуватися навіть для вчинення терористичних актів

Хакерські атаки відбуваються щодня, і здається, що в жодної організації немає від цього імунітету. З огляду на те, наскільки легко в сучасному світі зловмисники можуть викрадати і використовувати інформацію, зокрема персональні дані, в своїх цілях, занепокоєння про безпеку людей, процесів, даних і речей, підключених до Інтернету, цілком природно.

Отже захист інтересів держав та громадян в кіберпросторі стає життєво важливим завданням сьогодення.

Особливо безпечне користування Інтернетом стосується підростаючого покоління. Нині значна частина життя наших дітей «проходить» в Інтернеті, майже кожен учень має аккаунт в соціальній мережі, використовує Інтернет для навчання та розваг.

Про користь і шкоду цього можна сперечатися, але факт незаперечний: ми живемо в столітті інформації, проте навіть далеко не всі дорослі вміють правильно нею розпоряджатися, наприклад – захищати свої особисті дані надійним паролем. Діти і підлітки – дуже вразлива група. У всіх на слуху те, як дітей в соцмережах схиляють до самогубства, вербують в терористичні організації тощо.

Кібербезпека – дуже важливий аспект освіти сучасного учня, і навички грамотного поводження з інформацією треба формувати в школі.

В Законі України «Про основні засади забезпечення кібербезпеки України», який набрав чинності з 09.05.2018 р., зазначено, що кібербезпека – це «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».

«Стратегія кібербезпеки України» зазначає, що розвиток безпечного, стабільного і надійного кіберпростору має полягати в тому числі і завдяки «підвищенню цифрової грамотності громадян та культури безпечного поводження в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадженні державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту».

Велика кількість персональних даних потрапляє до комп’ютерних соцмереж. Важливо розуміти рівні захищеності власних даних, правила використання платіжних систем, наслідки, які можуть спричинити конфіденційні дані, що потрапили у відкритий доступ або у розпорядження кіберзлочинців.

Кіберзагрози існують повсюди, де застосовуються інформаційні технології, отже, вчитель будь-якого предмету та учень може в своїй діяльності зіткнутися і зі спамом, і з вірусами, і зі зломом комп'ютера і з

багатьма іншими проблемами, на які потрібно вміти не тільки оперативно реагувати, але і наскільки можливо вміти запобігати їх появі.

У сучасному шкільному курсі інформатики, нажаль, на вивчення такої важливої теми, як безпечне використання комп’ютерів та мережевих технологій відводиться не достатня кількість годин. За цей час можливо лише ознайомитись з основними поняттями про шкідливе програмне забезпечення та засобами боротьби з ним.

Навчальний курс за вибором (вибірковий модуль) «Вступ до кібербезпеки» (далі курс) протягом 2012-2018 навчальних років проходив апробацію у Навчально-виховному комплексі №141 ОРТ міста Києва, Навчально-виховному комплексі № 167 з поглибленим вивченням німецької мови міста Києва, Українському фізико-математичному ліцеї Київського Національного університету імені Тараса Шевченка, інших загальноосвітніх навчальних закладах України в яких працюють Мережні академії Cisco.

Курс передбачає детальне ознайомлення учнів із різноманітними методами кібербезпеки у сучасному кіберпросторі. Учні вивчають сучасні методики виявлення та усунення проблем безпеки. Завдяки вправам і лабораторним роботам учні зможуть налагоджувати програмні та апаратні засоби комп’ютерної та мережевої безпеки. Крім того, в навчальну програму включено розділи про навички мережевої комунікації.

Дана програма розроблена на основі курсу мережних академій Cisco Systems «Вступ до кібербезпеки» («Introduction to Cybersecurity»). Навчання за даною програмою надає учням базові знання в галузі комп'ютерної безпеки, необхідні для задоволення зростаючого попиту на фахівців з ІКТ початкового рівня. Курс охоплює відомості з основ безпеки роботи комп’ютерів та мереж, організації роботи мереж та ознайомлення з обов'язками фахівця з ІКТ.

Особливості курсу

Учні отримують теоретичні знання та практичні навички про безпечну роботу у комп'ютерних мережах, про те, як уникнути загроз пов’язаних зі спілкуванням у мережі, як зберегти особисті дані та захистити їх від зловмисників.

У курсі робиться акцент на практичному застосуванні навичок і процедур, необхідних для установки, оновлення обладнання та програмного забезпечення, а також пошуку та усунення шкідливого

програмного забезпечення. Практичні лабораторні заняття та віртуальні засоби навчання розвивають навички критичного мислення та вирішення складних завдань.

Виконання навчальних завдань на основі імітаційних моделей в середовищі програмного пакету Cisco Packet Tracer дозволяють учням експериментувати з проектами та конфігураціями мережі.

Інтерактивні атестації забезпечують негайний зворотний зв'язок для оцінки набутих компетенцій учня в даній предметній галузі.

Даний курс є початковою сходинкою до отримання професії і кар'єрного росту в сфері кібербезпеки. Органічним продовженням отримання професійної підготовки є інші куси, наприклад, Cybersecurity Essentials (Основи кібербезпеки) – вивчення фундаментальних принципів, процедур та методології мережевої та інформаційної безпеки; CCNA Cybersecurity Operations – Cisco Certified Networking Associate Cybersecurity Operations (Сертифікований Cisco мережевий спеціаліст – Операції з кібербезпеки) – отримання навичок в галузі кібербезпеки, які необхідні для роботи з глобальним загрозами, що безперервно розвиваються і удосконалюються; CCNA Security – Cisco Certified Networking Associate Security (Сертифікований Cisco мережевий спеціаліст – Безпека) – навчання проектувати, впроваджувати та підтримувати засоби забезпечення безпеки мережевих пристроїв.

Сертифікати курсів в області IT згідно з Болонською системою можуть використовуватися в якості бонусів при навчанні в університетах і коледжах за такими спеціальностями, як комп'ютерні науки та телекомунікації. Після закінчення кожного курсу є можливість скласти сертифікаційний іспит та отримати промисловий сертифікат. Учням, які успішно закінчили курси надаються певні знижки при здачі екзаменів на отримання промислових сертифікатів у спеціалізованих Центрах сертифікації.

Завдання курсу «Основи кібербезпеки» вдосконалення шкільної освіти і підготовки фахівців сфери безпеки в інформаційних технологіях, а також популяризація IT-професій.

Основною метою курсу є дослідження галузі кібербезпеки. У цьому курсі учні зможуть:

- дізнатися, як захищати в Інтернеті свої особисті дані та власну особистість;

● ознайомитись з різними типами шкідливого програмного забезпечення, кібератак та методами організації захисту від них;

● дізнатись про можливі варіанти кар'єри в галузі кібербезпеки;

● отримати загальні уявлення про безпеку в інформаційному суспільстві і на цій основі сформувати розуміння технологій інформаційної безпеки і вміння застосовувати правила кібербезпеки в усіх сферах діяльності.

Структура навчальної програми

Навчальна програма складається з таких розділів:

- Пояснювальна записка;
- Розподіл навчальних годин на вивчення тем програми;
- Критерії оцінювання навчальних досягнень учнів;
- Зміст навчального матеріалу та вимоги щодо рівня навчальних досягнень учнів;
- Додатки.

Курс складається з 5 модулів та розрахований на 17 годин. Для формування практичних навичок програмою курсу передбачено проведення ***8 практичних та лабораторних робіт.*** На виконання всіх робіт (практичних і лабораторних) передбачається **не більше 20 хвилин.** Вивчення кожного модуля закінчується ***контрольною роботою***, яку варто проводити у вигляді тестів в режимі реального часу також протягом 15-20 хвилин. Перед контрольною роботою бажано протягом 10-15 хвилин виконати вправи на терміни та принципи, які були вивчені в модулі.

Наприкінці курсу учні можуть скласти онлайн екзамен, що дає можливість отримати сертифікат про проходження курсу.

Модульна система курсу та виконання учнями контрольних робіт після кожного модуля дають можливість контролювати набуті учнями знання та навички як самостійно так і під час теоретичних занять, практичних і лабораторних робіт.

Курс розраховано на учнів 8-х – 11-х класів, які хочуть отримати професійні знання з основ сучасного підходу до кібербезпеки.

З метою полегшення користування даною навчальною програмою курсу подано критерії оцінювання навчальних досягнень учнів, деталізований перелік питань з кожної теми (модуля), що мають вивчатися та навчальні досягнення учнів, а також такі інформаційні матеріали:

- перелік додаткових навчально-методичних матеріалів курсу, які вчителі можуть використовувати під час роботи за програмою даного курсу (додаток 1);
- тлумачний словник термінів та абревіатур які зустрічаються у програмі (додаток 2);

Розподіл навчальних годин на вивчення тем програми

№ з/п	Зміст навчального матеріалу (Модулі)	Години
1.	Вступ.	1
2.	Модуль 1. Потреба в кібербезпеці.	3
3.	Модуль 2. Атаки, поняття та методи.	3
4.	Модуль 3. Захист даних і конфіденційність.	3
5.	Модуль 4. Захист організації.	3
6.	Модуль 5. Чи готові ви пов’язати своє майбутнє з кібербезпекою?	3
7.	Узагальнення та систематизація навчального матеріалу курсу. Отримання сертифікатів.	1
Усього годин.		17

Критерії оцінювання навчальних досягнень учнів

У наведеній нижче таблиці вказано критерії, за якими визначається рівень навчальних досягнень учнів з курсу. Кожному балу відповідає певний відсоток правильних відповідей учнів на контрольних роботах. Слід вважати, що знання, уміння та навички учня відповідають певному рівню навчальних досягнень, якщо вони відповідають критерію, вказаному для цього рівня, та критеріям для всіх попередніх рівнів.

Для отримання сертифікату по закінченні курсу учень має набрати під час тестування не менше 75% правильних відповідей, що відповідає достатньому рівню навчальних досягнень учнів.

Рівні навчальних досягнень	*Бали*	*Критерії оцінювання навчальних досягнень учнів*
І. Початковий	1	Учень (учениця): • розпізнає окремі об’єкти, явища і факти предметної галузі; • знає і виконує правила безпеки життєдіяльності під час роботи з комп’ютерною технікою Оцінка відповідає 39,9% суми правильних відповідей
	2	Учень (учениця): • розпізнає окремі об’єкти, явища і факти предметної галузі та може фрагментарно відтворити знання про них Оцінка відповідає 40-49,9% суми правильних відповідей

Рівні навчальних досягнень	*Бали*	*Критерії оцінювання навчальних досягнень учнів*
	3	Учень (учениця): • має фрагментарні знання незначного загального обсягу за відсутності сформованих умінь та навичок Оцінка відповідає 50-59,9% суми правильних відповідей
II. Середній	4	Учень (учениця): • має початковий рівень знань, значну (більше половини) частину навчального матеріалу може відтворити; • виконує елементарне навчальне завдання із допомогою вчителя; • має елементарні навички роботи на комп'ютері Оцінка відповідає 60-64,9% суми правильних відповідей
	5	Учень (учениця): • має рівень знань вищий, ніж початковий; • може з допомогою вчителя відтворити значну частину навчального матеріалу; • має стійкі навички виконання елементарних дій з опрацювання даних на комп'ютері Оцінка відповідає 65-69,9% суми правильних відповідей
	6	Учень (учениця): • пояснює основні поняття навчального матеріалу; • може самостійно відтворити значну частину навчального матеріалу; • вміє за зразком виконати просте навчальне завдання; • має стійкі навички виконання основних дій з опрацювання даних на комп'ютері Оцінка відповідає 70-74,9% суми правильних відповідей
III. Достатній	7	Учень (учениця): • вміє застосовувати вивчений матеріал у стандартних ситуаціях; • може пояснити основні процеси, що відбуваються під час роботи інформаційної системи, та наводити власні приклади на підтвердження деяких тверджень; • вміє виконувати навчальні завдання передбачені програмою. Оцінка відповідає 75-79,9% суми правильних відповідей.
	8	Учень (учениця) вміє: • аналізувати навчальний матеріал, в цілому самостійно застосовувати його на практиці; • контролювати власну діяльність; • самостійно виправляти вказані вчителем помилки; • самостійно визначати спосіб розв’язування навчальної задачі; • використовувати довідкові системи програмних засобів Оцінка відповідає 80-84,9% суми правильних відповідей.

Рівні навчальних досягнень	*Бали*	*Критерії оцінювання навчальних досягнень учнів*
	9	Учень (учениця): • вільно володіє навчальним матеріалом, застосовує знання на практиці; • вміє систематизувати і узагальнювати отримані відомості; • самостійно знаходить і виправляє допущені помилки; • може аргументовано обрати раціональний спосіб виконання навчального завдання; • використовує електронні засоби для пошуку потрібної інформації. Оцінка відповідає 85-89,9% суми правильних відповідей.
IV. Високий	10	Знання, вміння і навички учня відповідають вимогам програми у повному обсязі. Учень (учениця): • володіє міцними знаннями, самостійно визначає проміжні етапи власної навчальної діяльності, аналізує нові факти, явища; • вміє самостійно знаходити додаткові відомості та використовує їх для реалізації поставлених перед ним навчальних завдань, судження його логічні і достатньо обґрунтовані; • має сформовані навички керування інформаційними системами. Оцінка відповідає 90-92,9% суми правильних відповідей.
	11	Учень (учениця): • володіє узагальненими знаннями з курсу; • вміє планувати особисту навчальну діяльність, оцінювати результати власної практичної роботи; • вміє самостійно знаходити джерела різноманітних відомостей і використовувати їх відповідно до мети і завдань власної пізнавальної діяльності; • використовує набуті знання і вміння у нестандартних ситуаціях; • вміє виконувати завдання, не передбачені навчальною програмою; • має стійкі навички керування інформаційними системами. Оцінка відповідає 93-96,9% суми правильних відповідей.
	12	Учень (учениця): • має стійкі системні знання та творчо їх використовує у процесі продуктивної діяльності; • вільно опановує та використовує нові інформаційно-комунікаційні технології для поповнення власних знань та розв'язування задач; • має стійкі навички керування інформаційними системами в нестандартних ситуаціях. Оцінка відповідає 97-100% суми правильних відповідей.

Зміст навчального матеріалу та вимоги щодо рівня навчальних досягнень учнів

Очікувані результати	Зміст навчання
Потреба в кібербезпеці (3 години)	
Знаннєва складова Пояснює, що таке кібербезпека. Знає хто такі кібер-нападники і яка їхня мета. Знає на які види поділяють хакерів та типи порушників у сфері кібербезпеки. Знає і пояснює, що таке онлайн-ідентифікація та що таке дані, де вони знаходяться і чому це цікавить кібер-злочинців. Знає та розуміє наслідки порушення кібербезпеки, розрізняє внутрішні та зовнішні загрози. Має поняття кібервійни. Знає та розуміє основні правові проблеми кібербезпеки. **Діяльнісна складова** Обчислює хеш для файлу та використовує хеш-значення, щоб перевірити цілісність файлу. Вживає елементарні заходи з безпеки при роботі у мережі Інтернет. **Ціннісна складова**	Поняття кібербезпеки. Онлайн та офлайн ідентифікація. Приватні дані та місця їх розташування. Причини викрадення даних. Типи даних організації. Конфіденційність, цілісність та доступність даних. Наслідки порушення безпеки. Типи порушників у сфері кібербезпеки. Внутрішні та зовнішні загрози. Правові проблеми кібербезпеки. Поняття про хешування даних. Етичні питання кібербезпеки. кібервійни. *Практичні роботи: Хешування даних*

Усвідомлює важливість кібербезпеки. Розуміє, чому зростає попит на фахівців з кібербезпеки. При роботі у мережі демонструє етичну поведінку. Розуміє і уявляє наслідки кібервійни і чому країни та уряди потребують фахівців з кібербезпеки, щоб захистити своїх громадян та інфраструктуру.	
Атаки, поняття та методи	
Знаннєва складова Наводить приклади вразливостей програмного та апаратного забезпечення. Знає найпоширеніші симптоми шкідливого програмного забезпечення. Пояснює поняття «соціальна інженерія» та види атак соціальної інженерії. Знає методи зламу паролю Wi-Fi. Розрізняє типи мережних атак. Розуміє що таке змішані атаки. **Діяльнісна складова** Розрізняє категорії вразливостей програмного забезпечення. Уміє розрізняти типи шкідливих програм. Розрізняє методи (способи) проникнення в систему (соціальна інженерія, злам пароля Wi-Fi, використання вразливості).	Пошук вразливостей безпеки. Вразливості програмного забезпечення та апаратного забезпечення. Класифікація вразливостей безпеки. Ідентифікація категорій вразливостей. Типи шкідливого програмного забезпечення: шпигунські програми, рекламне програмне забезпечення, боти, програми-вимагачі, псевдоантивіруси, руткіти, віруси, троянські коні, черв'яки, людина посередині, посередник у мобільному телефоні. Симптоми шкідливого програмного забезпечення. Визначення типів шкідливих програм. Соціальна інженерія. Злам паролю Wi-Fi. Використання вразливості. Типи мережних атак. Змішані атаки. Запобігання нападу на систему та зменшення наслідків нападу. Зменшення впливу атаки. Роль фахівця з кібербезпеки в сучасному інформаційному суспільстві.

Уміє визначати тип атаки (DoS, DDoS, отруєння SEO). **Ціннісна складова** Має уявлення про можливості запобігання нападу на систему та зменшення наслідків нападу, коли атаці неможливо запобігти. Усвідомлює важливість заходів, які потрібно вжити, коли виявлено порушення безпеки. Оцінює роль робота фахівця з кібербезпеки в сучасному інформаційному суспільстві.	
Захист даних і конфіденційність	
Знаннєва складова Знає про захист пристроїв. Знає як створити надійний пароль і безпечно використовувати бездротові мережі. Має поняття про методи аутентифікації, які допоможуть безпечно зберігати дані. Знає, що можна робити в Інтернеті, а чого робити не варто. Знає про деякі способи захисту даних у онлайн сервісах. Володіє базовою термінологією, що стосується кібербезпеки. **Діяльнісна складова** Може виконати елементарні дії для захисту комп'ютерних пристроїв від вторгнення. Вміє створювати надійні паролі. Має навички роботи з веб-сканером IoT пристроїв Shodan.	Захист комп'ютерних пристроїв від стороннього вторгнення. Безпечне використання бездротових мереж. Правила створення та використання паролів. Шифрування даних. Створення резервних копій даних. Повне видалення даних. Двофакторна аутентифікація. OAuth 2.0. Правила роботи в соціальних мережах. Конфіденційність електронної пошти та веб-браузера. *Практичні роботи:* Створення та збереження надійних паролів. Резервне копіювання даних на зовнішній накопичувач. Хто володіє вашими даними? Дослідження ризиків своєї поведінки в Інтернеті.

Може зашифрувати дані за допомогою EFS. Вміє здійснювати резервне копіювання даних. **Ціннісна складова** Усвідомлює про безпечність збереження особових даних. Знає і використовує ресурси, що мають двофакторну аутентифікацію для надійного зберігання даних. Розуміє і знає про небезпеку соцмереж, та знає як уникнути цього ризику для безпеки	
Захист організації	
Знаннєва складова Знає про деякі технології та процеси захисту мережі, обладнання та даних організації. Пояснює про бот-мережі, ланцюжок знищення, безпеку на основі аналізу поведінки та використання NetFlow для моніторингу мережі. **Діяльнісна складова** Описує різні типи фаєрволів, пристроїв безпеки та програмного забезпечення, які на даний час використовуються. Може виявляти атаки безпеки у реальному часі. Може вмикнути фаєрвол. Вміє сканувати порти. **Ціннісна складова** Усвідомлює поведінковий підхід до кібербезпеки. Знає найкращі практики безпеки.	Файєрволи та їх типи. Визначення типу файєрволу. Сканування портів. Пристрої безпеки. Визначення пристроїв безпеки. Виявлення атак у реальному часі. Захист від шкідливого програмного забезпечення. Найкращі практики безпеки. Поведінковий підхід до кібербезпеки. Ботнет. Вбивчий ланцюг (проникнення в кіберзахист). Безпека на основі аналізу поведінки. NetFlow та кібератаки. Команди комп'ютерної безпеки з реагування на інциденти. Підхід Cisco до кібербезпеки. Інструменти для запобігання та виявлення інцидентів.

Знає інструменти для запобігання та виявлення інцидентів.	
Чи готові ви пов’язати своє майбутнє з кібербезпекою?	
Знаннєва складова Знає структуру сертифікації та може отримати доступ до опису деталей всіх видів сертифікації. Знає про освітні напрямки, які може пройти для отримання сертифікатів Мережної академії Cisco. Розрізняє різні види професій повязаних із кібербезпекою. **Діяльнісна складова** Знає та вміє здійснювати пошук відповідних вакансій та матеріалів для навчання. Може написати резюме та підготуватися до співбесіди під час прийому на роботу. **Ціннісна складова** Знає та розуміє важливість роботи кіберзахисників. Може зробити вмотивований вибір професії повязаної із кібербезпекою.	Освіта та кар’єра в галузі кібербезпеки. Можливості сертифікації. Можливості працевлаштування. Вакансії з кібербезпеки. *Практичні роботи:* Створення резюме та підготовка до співбесіди під час прийому на роботу. Пошук матеріалів для навчання. Пошук вакансій з кібербезпеки.

Додаток 1

Перелік додаткового навчально-методичного забезпечення, яке можна використати під час навчання за програмою курсу, та його короткий опис

Номер модуля	Назва відеоролику	Опис
1	«Що таке кібервійна?»	Кіберпростір став ще одним важливим аспектом війни, де країни можуть конфліктувати без зіткнення традиційних військ та техніки. Це дозволяє країнам з мінімальними військовими силами бути такими ж сильними, як і інші країни в кіберпросторі. Кібервійна – це Інтернет-конфлікт, який передбачає проникнення у комп'ютерні системи та мережі інших країн. Нападники мають ресурси та спеціальні знання, щоб започатковувати масштабні інтернет-атаки проти інших країн, завдаючи збитків або порушуючи роботу сервісів, наприклад, припинення роботи енергосистеми.
4	«Інструменти для запобігання та виявлення інцидентів».	Відео про інструменти, що використовуються для запобігання та виявлення інцидентів.
5	«Можливості сертифікації».	Мережна академія Cisco пропонує багато курсів, які допоможуть вам підготуватися як до сертифікаційних іспитів Cisco, так і до інших сертифікаційних іспитів. Перегляньте відео «Станьте кібер-героєм».

Додаток 2

Тлумачний словник термінів та абревіатур які зустрічаються у програмі

1) індикатори кіберзагроз - показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;
2) інформація про інцидент кібербезпеки - відомості про обставини кіберінциденту, зокрема про те, які об’єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;
3) інцидент кібербезпеки (далі - кіберінцидент) - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;
4) кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту;
5) кібербезпека - 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;
6) кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;
7) кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;
8) кіберзлочин (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;
9) кіберзлочинність - сукупність кіберзлочинів;
10) кіберпростір - 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;
11) кібертероризм - терористична діяльність, що здійснюється у кіберпросторі або з його використанням;
12) кібершпигунство - шпигунство, що здійснюється у кіберпросторі або з його використанням;
13) національні електронні інформаційні ресурси (далі - національні інформаційні ресурси) - систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;
14) системи електронних комунікацій (далі - комунікаційні системи) - системи передавання, комутації або маршрутизації, обладнання та інші ресурси

(включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв’язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв’язку, комп’ютери, інша комп’ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних.