ЧАСТИНА І. ТЕОРЕТИЧНІ ВІДОМОСТІ

Тема 1. Загальні правила безпечної роботи з пристроями та програмами

Понятійний апарат у сфері кібергігієни

План лекції

Вступ
1. Що таке кібергігієна?
2. Що таке кібербезпека?
3. Що таке інформаційна безпека?

Висновки

Рекомендована література
Основна

1. Даник Ю.Г., Грищук Р.В. Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ, 2016. 636 с.
2. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків: Промарт, 2020. 162 с. з іл. URL: https://univd.edu.ua/science-issue/issue/4315.
3. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 106 с.
4. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К. : ВАІТЕ, 2021. 262 с.

Допоміжна

5. Манжай О.В., Манжай І.А. Що таке кібергігієна? // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків : ХНУВС, 2021. С. 65–67.
6. Носов В.В., Манжай О.В. Зміст та методологія практичного навчання з питань кібергігієни // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків: ХНУВС, 2021. С. 72–73.
7. Про критичну інфраструктуру: Закон України від 16.11.2021. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.
8. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
9. Про створення Центру протидії дезінформації: Рішення Ради національної безпеки і оборони України від 11.03.2021, введено в дію Указом Президента України від 19.03.2021 № 106/2021. URL: https://zakon.rada.gov.ua/laws/show/106/2021#Text.

10. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.
11. Стратегія кібербезпеки України, затверджена Указом Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.
12. Maennel K., Mäses S., Maennel O. Cyber Hygiene: The Big Picture. In: Gruschka N. (eds) Secure IT Systems. NordSec 2018. *Lecture Notes in Computer Science.* 2020. Vol. 11252. Springer, Cham. (DOI: 10.1007/978-3-030-03638-6_18).
13. Pfleeger S. L., Sasse M. A., Furnham A. From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Journal of Homeland Security and Emergency Management.* 2014. Vol. 11. Iss. 4. pp. 489–510. (DOI: 10.1515/jhsem-2014-0035).
14. Review of cyber hygiene practices (December 2016). European Union Agency For Network and Information Security (ENISA). https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport, p. 4.
15. Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J. Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems.* 2020. Vol. 128 (DOI: 10.1016/j.dss.2019.113160).

Інформаційні ресурси в Інтернеті

16. Освітній серіал «Основи кібергігієни». URL: https://osvita.diia.gov.ua/courses/cyber-hygiene.

Текст лекції

Вступ

Сьогодні безпека роботи з інформацією є актуальною як ніколи. Зростаючі кібератаки на державні та приватні підприємства, установи й організації тільки посилюють цей тренд. Окрема категорія загроз стосується громадян, які все частіше стають об'єктом прискіпливої уваги правопорушників. Враховуючи це, поступово набуває поширення відносно нова концепція необхідності самостійного дотримання користувачами елементарних правил безпеки. Такий підхід дає змогу значно посилити систему колективної безпеки суспільства та держави в цілому. Агентство Європейського Союзу з мережевої та інформаційної безпеки (European Union Agency for Network and Information Security) відзначає, що кібергігієна повинна розглядатися так само, як і особиста гігієна, й після належної інтеграції в організацію стати простою повсякденною процедурою, яка забезпечить стан кіберздоров'я організації на оптимальному рівні.

Порушення правил кібергігієни може призвести для згубних наслідків не лише для окремої людини. Досить часто від дій зловмисників страждає і роботодавець жертви. Навіть великі держави можуть зазнати величезної шкоди від необачного ставлення до вимог безпеки однієї людини. Часто порушники використовують окрему особу як лаз для проникнення на об'єкти критичної інфраструктури, викрадення чутливих державних даних, створення умов для скоординованих повномасштабних атак.

Таким чином, недотримання вимог кібергігієни здатне нанести значну матеріальну та моральну шкоду. А, крім того, ще й істотно вплинути на вашу особисту репутацію!

1. Що таке кібергігієна?

У світі існує достатньо велика кількість тлумачень слова «кібергігієна». Вони, як правило, відображають найбільш значущі аспекти цього терміна, важливі для конкретної галузі знань. Серед останніх оприлюднених визначень можна навести такі:

- правила кібербезпеки, яких мають дотримуватися онлайн-користувачі з метою забезпечення цілісності та убезпечення своїх персональних даних на мережевих пристроях від компрометації у випадку кібератаки;
- сукупність практик, спрямованих на захист від негативного впливу на певні об'єкти ризиків, пов'язаних з кібербезпекою;
- способи заохочення користувачів комп'ютерних технологій до безпечної поведінки в Інтернеті.

Більш спрощена інтерпретація цього терміна дозволяє представити кібергігієну як дотримання правил безпечної поведінки у кіберсфері.
Така поведінка обумовлена наявністю загроз, які виникають під час роботи користувачів з інформацією в електронному вигляді. Спроби реалізації загроз називаються атаками.

Як і на рибалці або полюванні, зловмисники можуть заздалегідь обирати цілі, які вважають цікавими для себе, а можуть навпаки – розставити пастки й чекати, доки жертва потрапить в одну з них. Те саме стосується ситуацій, коли порушники випадковим чином обирають жертву, стосовно якої намагаються реалізувати свої наміри.

Виділяють кілька типів *інформаційних атак:* соціальна інженерія, одержання віддаленого доступу за допомогою вірусів, вплив на інфраструктуру стільникового зв'язку, маніпуляція через ЗМІ, атаки відмови в обслуговуванні, атаки на енергетичні системи та комунікації, політичний спамінг, атаки на системи управління та провайдерів тощо.

Перед тим, як напасти, зловмисниками можуть здійснюватися підготовчі дії. Це дістає вияв у підшукуванні працездатних схем нападу, збиранні інформації про жертву різними способами, створенні умов для реалізації атаки.

Для того, щоб мінімізувати ризик успішної реалізації таких атак, саме і потрібна кібергігієна. По суті, це – рутинний процес. І з тим, щоб його полегшити, потрібно використовувати допоміжний інструментарій. Якщо у класичній гігієні такими інструментами є мило, шампунь, зубна щітка тощо, то для забезпечення її кібернетичного аналогу використовуються спеціальні програми: антивіруси, фаєрволи, захищені браузери та багато інших застосунків і сервісів.

Важливим моментом в роботі з інструментами кібергігієни є правильне їх застосування. Це приблизно те саме, що і правильне підрізання нігтів ножицями або зачісування волосся гребінцем. З одного боку, все просто, а з іншого – потрібно чітко визначити для себе елементарний порядок дій з певними програмами, щоб не вскочити у халепу. Просте озброєння купою застосунків для захисту інформації, як правило, не приносить користі. Без знання правил роботи з такими програмами вони стають просто набором коду, який навряд чи зможе вас захистити.

Так само потрібно мати на увазі, що чим меншою буде кількість інформації, яку ви хочете вберегти, тим менше вам потрібно буде вживати дій для її убезпечення. Тому під час продукування фотознімків, написання повідомлень у мережі, спілкування телефоном з незнайомими – та й навіть зі знайомими людьми подумайте, чи дійсно це є необхідним, і наскільки шкідливим може бути використання відповідної інформації проти вас.

Саме тому бажано користуватися перевагами Інтернету в частині забезпечення анонімності та використання вигаданих даних. Особливо це стосується мережевих ресурсів, у безпеці яких не можна бути впевненим. У випадку атаки на вас зловмисники зможуть отримати доступ лише до вигаданих даних. Це може стати ще одним додатковим ешелоном, що убезпечить вас від протиправних посягань.

Немаловажним принципом забезпечення кібергігієни є періодичне резервування даних. Можна використовувати мережеве резервування або дублювання даних на фізичних запам'ятовувальних пристроях. Усе залежить від чутливості даних, які потрібно зберегти, та відповідних знань предметного характеру. Так, наприклад, другорядні дані цілком можуть бути перенесені у хмару. Це дозволить зменшити кількість інформації, що потребує захисту на локальних пристроях, і, таким чином, тримати їх у чистоті.

Найкращий варіант – якщо ви зробите кібергігієну своєю повсякденною звичкою. При цьому вона не потребує суттєвих витрат коштів і часу. Згодом ви звикнете до виконання відповідних процедур і відчуєте їх корисність як в особистих, так і в службових справах.

Тісно пов'язаними з кібергігієною є поняття «кібербезпека» та «інформаційна безпека».

2. Що таке кібербезпека?

У Законі України від 05.10.2017 «Про основні засади забезпечення кібербезпеки України» **кібербезпека** визначається 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.

Актуальні загрози кібербезпеці та шляхи їх блокування викладено у підзаконних актах. Наприклад, ***Стратегія кібербезпеки України*** – це документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Докладніше структуру вказаного документа зображено на рис. 1.

Рис. 1. Основні елементи стратегії кібербезпеки України

Об'єктами кібербезпеки є:

1) конституційні права і свободи людини і громадянина;
2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;
3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;
4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;
5) об'єкти критичної інфраструктури.

Цікавим нововведенням Стратегії кібербезпеки стало запровадження відповідних маркованих літерно-числовими ідентифікаторами стратегічних цілей (табл. 1).

Таблиця 1. Потенціал та стратегічні цілі кібербезпеки

ПОТЕНЦІАЛ ЦІЛІ	СТРИМУВАННЯ **(С)**	КІБЕРСТІЙКІСТЬ **(К)**	УДОСКОНАЛЕННЯ ВЗАЄМОДІЇ **(В)**
1	*Дієва кібероборона*	*Національна кіберготовність та надійний кіберзахист*	*Зміцнення системи координації*
2	*Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму*	*Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки*	*Формування нової моделі відносин у сфері кібербезпеки*
3	*Ефективна протидія кіберзлочинності*	*Безпечні цифрові послуги*	*Прагматичне міжнародне співробітництво*
4	*Розвиток асиметричних інструментів стримування*		

Для досягнення виділених цілей передбачено виконання цілої низки завдань. Так, наприклад, для досягнення цілі К.1 Україна у співпраці із суб'єктами приватного сектору, академічною спільнотою та громадськістю забезпечить посилення національної кіберготовності та кіберзахисту шляхом:

- розроблення Національного плану реагування на надзвичайні (кризові) ситуації в кіберпросторі, який визначить механізми реагування на кібератаки загальнонаціонального масштабу щодо об'єктів критичної інформаційної інфраструктури та заходи з подальшого відновлення;
- створення національної системи управління інцидентами, розроблення та впровадження стандартних операційних процедур для реагування на різні види подій у кіберпросторі з визначенням критеріїв для оцінки критичності подій та пріоритетності реагування залежно від визначеного рівня критичності;
- забезпечення постійного моніторингу національних електронних комунікаційних мереж та інформаційних ресурсів, аналізу вторгнень щодо цих мереж і ресурсів, а також виявлення в режимі реального часу аномалій їх функціонування;
- запровадження планування видатків на кібербезпеку за окремими бюджетними програмами;

- розроблення базових (визначатимуть мінімальний обов'язковий рівень) вимог та рекомендацій з питань забезпечення кібербезпеки для державного і приватного секторів з урахуванням кращих світових практик;
- налагодження на основі взаємної довіри системного обміну інформацією про кібератаки, кіберінциденти та індикатори кіберзагроз між усіма суб'єктами забезпечення кібербезпеки, насамперед на базі технологічної платформи Національного координаційного центру кібербезпеки, уніфікації форматів обміну інформацією;
- впровадження ризик-орієнтованого підходу стосовно заходів забезпечення кібербезпеки об'єктів критичної інфраструктури та державних органів, зокрема, розроблення методики ідентифікації та оцінки кіберризиків на національному рівні та для секторів критичної інфраструктури держави, врегулювання на законодавчому рівні обов'язковості здійснення періодичного оцінювання ризиків на підставі розроблених методик;
- впровадження системи сертифікації продукції, яка використовується для функціонування та кіберзахисту інформаційно-комунікаційних систем, насамперед об'єктів критичної інформаційної інфраструктури;
- забезпечення розвитку організаційно-технічної моделі кіберзахисту;
- завершення процесів визначення об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, створення і забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури, постійного перегляду та оновлення вимог щодо їх кіберзахисту з урахуванням сучасних міжнародних стандартів з питань кібербезпеки;
- запровадження на постійній основі оцінювання стану захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на вразливість, встановлення обов'язковості та періодичності проведення такого оцінювання з урахуванням категорій критичності об'єктів, стимулювання участі у цих заходах фахівців з кібербезпеки приватного сектору;
- впровадження системи аудиту інформаційної безпеки, насамперед на об'єктах критичної інфраструктури, визначення механізмів та базових методик проведення аудитів, встановлення вимог до аудиторів інформаційної безпеки, їх сертифікації, атестації (переатестації), навчання та підвищення кваліфікації, а також щодо обов'язковості та періодичності проведення аудитів, надання узагальненої інформації про результати аудитів до Національного координаційного центру кібербезпеки;
- забезпечення розвитку систем технічного і криптографічного захисту інформації, пріоритетності використання засобів технічного і криптографічного захисту інформації вітчизняного виробництва для кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури;
- впровадження вітчизняних рішень із захисту інформації;

- проведення командно-штабних кібернавчань стратегічного рівня, а також тематичних кібернавчань та тренінгів за участю представників державного та приватного секторів;
- забезпечення розвитку мережі центрів реагування на кібератаки та кіберінциденти;
- завершення розгортання Національної телекомунікаційної мережі, збільшення її пропускної здатності, передбачення під час її функціонування використання винятково вітчизняних засобів криптографічного захисту інформації;
- забезпечення функціонування та розвитку Національного центру резервування державних інформаційних ресурсів, проведення модернізації системи захищеного доступу державних органів до мережі Інтернет;
- створення національного сервісу доменних імен (DNS).

Крім розглянутих документів, існує ціла низка відповідних методичних рекомендацій, які, хоч і не є обов'язковими до виконання, проте можуть бути використані під час побудови системи кіберзахисту. Так, Адміністрація Держспецзв'язку наказом від 06.10.2021 № 601 затвердила Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Рекомендації розроблені з урахуванням Настанови для підвищення кібербезпеки критичної інфраструктури (Framework for Improving Critical Infrastructure Cybersecurity), виданої у 2014 році та оновленої у 2018 році Національним інститутом стандартів і технології Сполучених Штатів Америки (National Institute of Standards and Technology).

3. Що таке інформаційна безпека?

15 жовтня 2021 року Рада національної безпеки та оборони України розглянула та схвалила Стратегію інформаційної безпеки, проект якої був внесений Кабінетом Міністрів України.

Результатами реалізації Стратегії мають стати:

- захищений інформаційний простір;
- ефективне функціонування системи стратегічних комунікацій;
- ефективна протидія поширенню незаконного контенту;
- інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України;
- підвищення рівня медіакультури та медіаграмотності населення;
- забезпечення захисту прав журналістів;
- формування загальнонаціональної ідентичності.

Згідно з положеннями Стратегії інформаційної безпеки *інформаційна безпека України* – це складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності,

демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії завданню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом.

Серед іншого, в документі наводиться аналіз головних викликів та загроз (рис. 2).

Рис. 2. Загрози та виклики інформаційній безпеці

Основними напрямами забезпечення інформаційної безпеки України є стійкість та взаємодія, для досягнення яких необхідним є виконання семи стратегічних цілей (рис. 3) та низки завдань.

Так, наприклад, для досягнення цілі підвищення рівня медіакультури та медіаграмотності суспільства потрібно виконати такі завдання:

- підготовка та проведення просвітницької кампанії з медіаграмотності, що включатиме такі компоненти, як розвиток критичного мислення, навички перевірки фактів і визначення маніпуляційних технік, ознайомлення з найпоширенішими порушеннями прав людини із застосуванням інтернет-технологій тощо;
- створення сприятливих умов для здійснення діяльності засобів масової інформації;
- створення сприятливих умов для підвищення рівня професійної підготовки медіафахівців;
- удосконалення законодавства у сфері реклами, зокрема щодо лібералізації норм у цій сфері та посилення відповідальності за трансляцію прихованої реклами;
- стимулювання розвитку соціально відповідального бізнесу серед засобів масової інформації.

Рис. 3. Стратегічні цілі забезпечення інформаційної безпеки

Механізми реалізації окресленої мети та завдань визначаються через уповноваження відповідних суб'єктів (рис. 4) на здійснення заходів щодо забезпечення інформаційної безпеки.

Рис. 4. Суб'єкти забезпечення інформаційної безпеки

Виходячи з наведеного, нескладно побачити, що інформаційна безпека, на відміну від кібербезпеки, більшою мірою стосується убезпечення інформаційного простору від різних загроз, у тому числі під час здійснення інформаційної війни.

Висновки

Підсумовуючи, окреслимо деякі головні правила кібергігієни:

1. Завжди критично ставтеся до відомостей, одержаних з мережі Інтернет.
2. Регулярно здійснюйте резервування важливих даних, не зберігайте все в одному місці.
3. Намагайтеся користуватися останніми версіями програмного забезпечення та регулярно виконуйте оновлення.
4. Залишайте якомога менше персональних даних у мережі Інтернет.
5. Дотримуйтесь вимог парольного захисту та використовуйте за можливості багатофакторну автентифікацію.
6. Користуйтеся антивірусним програмним забезпеченням та іншими засобами убезпечення.
7. У випадку компрометації чутливих даних повідомте про це уповноважену особу та вживайте заходів убезпечення решти відомостей.
8. Максимально обмежте доступ сторонніх осіб до терміналів, за якими ви працюєте.
9. Використовуйте тільки перевірені носії інформації.
10. Регулярно оновлюйте знання у сфері кібергігієни.