Кібербезпека та захист даних

Ставицький Сергій Борисович,
завідувач Центру медіа та інформаційних технологій,
викладач секції інформаційних технологій в освіті
КВНЗ «Харківська академія неперервної освіти»

Вітаємо на занятті з кібербезпеки!

Під час знайомства з матеріалами ви дізнаєтеся:

- що таке цифровий простір і кібербезпека, кібератаки і кібертероризм;
- про особливості реалізації атак і заходи з послаблення їхнього деструктивного впливу;
- про загальні вимоги до кібербезпеки та різні її типи;
- про комп’ютерні віруси, їх класифікацію та захист;
- правила кібергігієни.

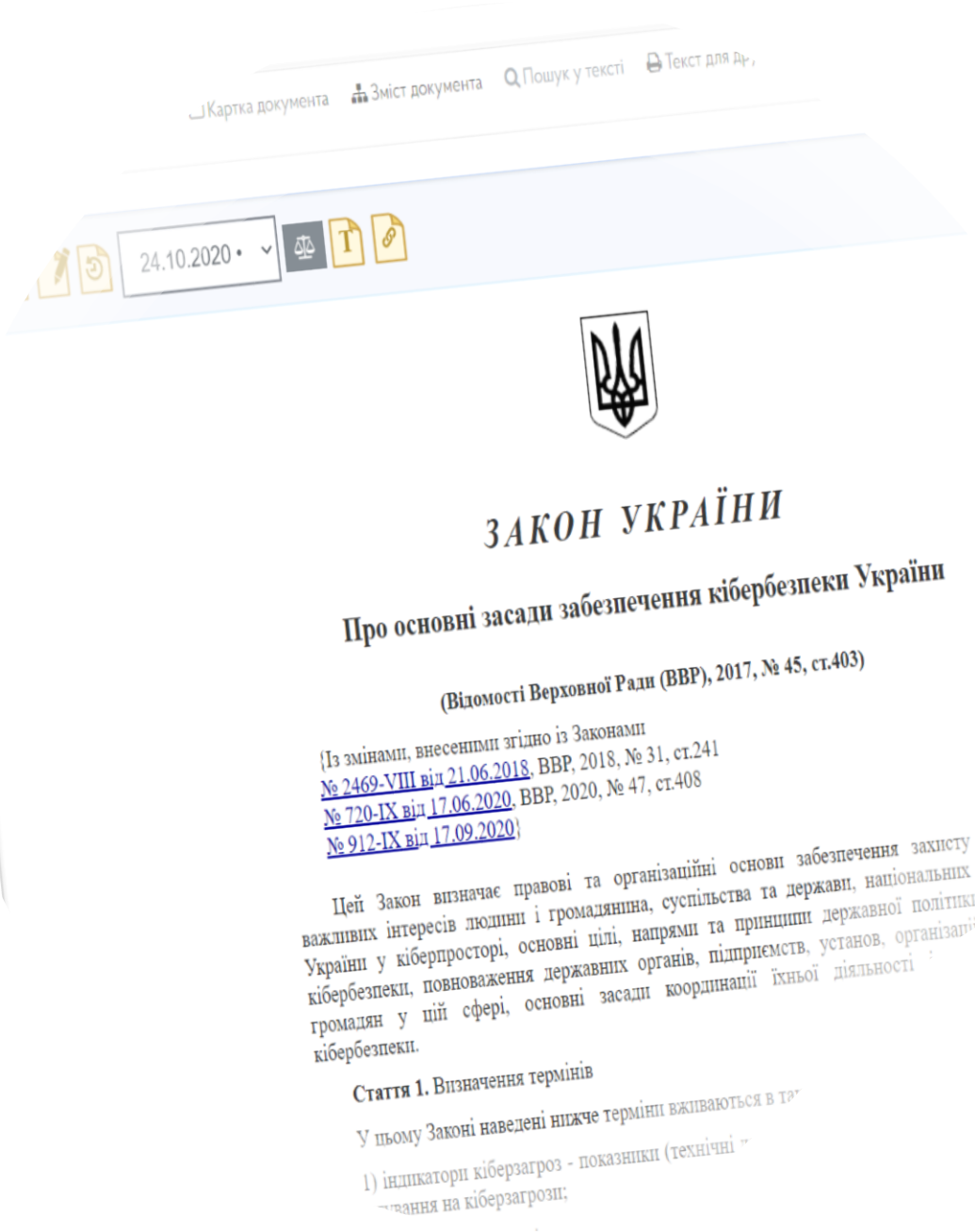
Розглянемо перше питання:

Що таке кіберпростір і кібербезпека?

Люди живуть та діють у цифровому просторі (ЦП). Діти народжуються, зростають, навчаються і працюватимуть з гаджетами, що під'єднані до мереж і стають природним середовищем. Їх життя знаходиться під впливом і дією ЦП зі старими та новими небезпеками, залежить все більше від когнітивних факторів (інтерфейсу, вмісту, моделей поведінки) і може характеризуватися з позицій безпеки, ефективності та комфортності (зокрема здоров'я), тобто знаходиться в полі діяльності ергономістів.

Під впливом новітніх інформаційних технологій відбуваються процеси трансформації суспільного розвитку настільки фундаментальні й глобальні, що, крім позитивного впливу, закономірно несуть з собою серйозні проблеми, загрози і ризики в разі недооцінки нових факторів і умов.

Як відзначалось у матеріалах Міжнародних Форумів у Давосі (2018–2019 рр.), особливої гостроти набуває проблема кібербезпеки (КБ), яка стосується практично всіх сфер життя та діяльності людини.



Поняття кіберпростору

Як визначається Законом **“Про основні засади забезпечення кібербезпеки України”**, «*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».

Звертається увага на те, що кіберпростір визначається різноманіттям з'єднань, що одночасно переводить його в категорію зони ризику.

Кіберпростір

Кіберпростір можна розглядати як тріаду, до якої входять:

1) *інформація* у своєму цифровому представленні: статична (файли, записані на носії інформації) та динамічна (пакети, потоки, команди, запити тощо);
2) *технічна інфраструктура*: ІКТ, програмне забезпечення, бази даних та бази знань;
3) *інформаційна взаємодія* суб'єктів з використанням отриманої (переданої) інформації та обробки через технічну інфраструктуру.

Цифровий простір: як технології змінять наш стиль життя

Прогноз #1: Суспільство висуває вимоги до пристроїв, компанії адаптуються

Розумна інфраструктура міста, розумний будинок, цифровий робочий простір - це все приклади екосистем, в яких люди і пристрої взаємодіють один з одним.

Розпізнавання голосу, аутентифікація за допомогою фото, відбитка пальця, постійне підключення до мережі разом з категорією смарт-дисплеїв, що розвивається, змінять наше уявлення як про взаємодію з технікою, так і між собою.

Зміниться ситуація і на робочому місці. Визначальним фактором розвитку технологій буде взаємодія покоління міленіалів і пост-міленіалів, які активно використовують планшети, а також технології доповненої і віртуальної реальності.

Цифровий простір: як технології змінять наш стиль життя

Прогноз #2: Технології у сферах, з якими ми взаємодіємо щодня

Інтернет речей (IoT), штучний інтелект (AI) і доповнена/віртуальна реальність (AR/VR) - технології, які будуть поступово впроваджуватися в різноманітні сфери життя: виробництво, освіту, рітейл, медицину.

В Україні технології віртуальної реальності активно використовуються в освіті.

На початку 2019 року Академія ДТЕК впровадила систему віртуального навчання співробітників.

Цифровий простір: як технології змінять наш стиль життя

Прогноз #3: Технології доповненої і віртуальної реальності відходять від функції розваг

Доповнена реальність буде активно використовуватися не тільки для розваг, а й для навчання, в комерційних цілях і навіть у віртуальному туризмі.

Ви тільки уявіть, що завдяки технологіям віртуальної реальності, не виходячи з дому, ви можете не просто побачити незвичайні місця у місті, а й зазирнути за лаштунки театру, відчути себе конструктором легендарних українських велосипедів "Еней" або диригувати оркестром.

На початку 2019 року Академія ДТЕК впровадила систему віртуального навчання співробітників.

Цифровий простір: як технології змінять наш стиль життя

Прогноз #4: Штучний інтелект змінить уявлення про цифрову безпеку

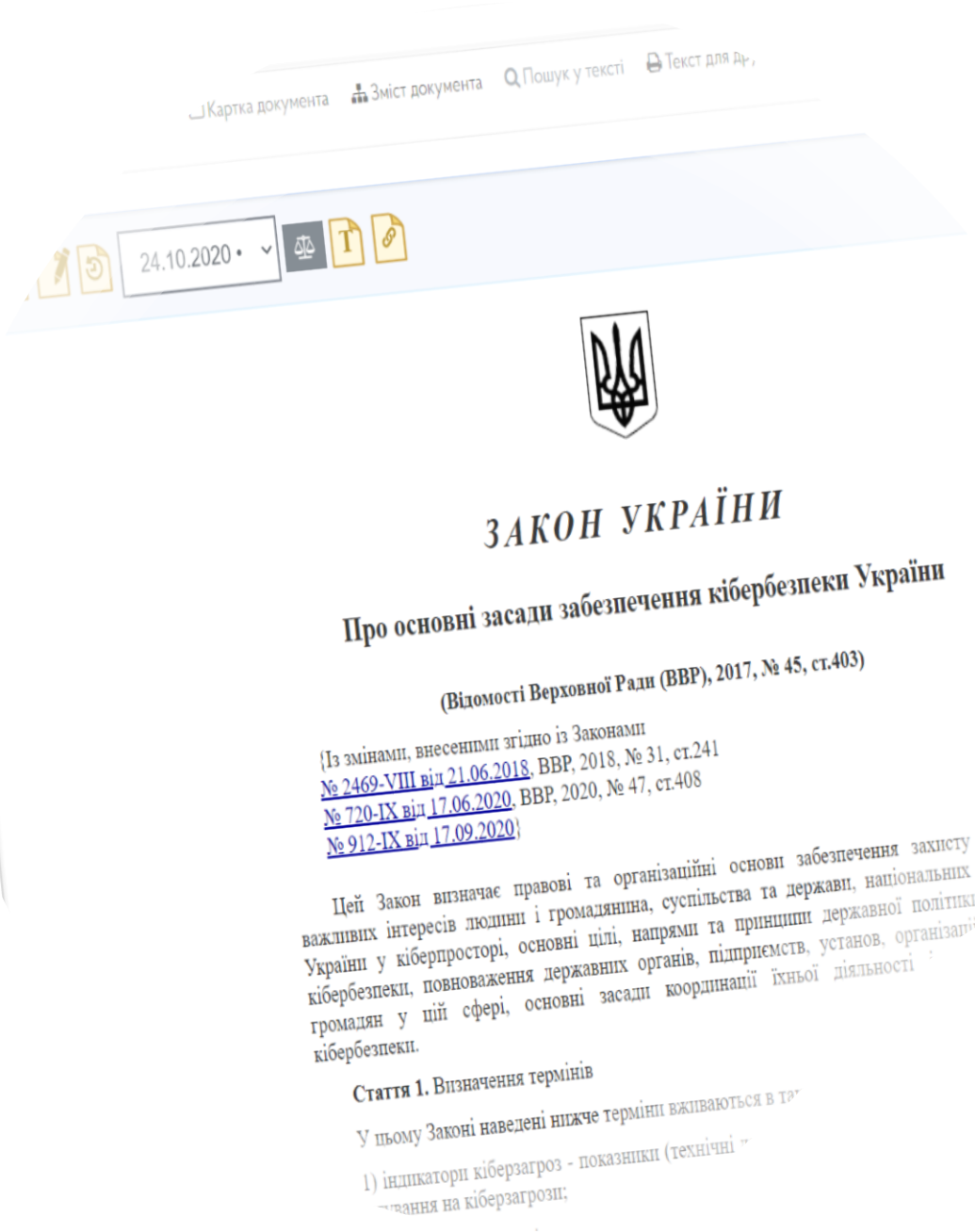
Людський фактор – найслабша ланка в безпеці інформації не тільки в Україні, але у всьому світі.

Співробітники, які не знають основ цифрової безпеки або не надають їй великого значення, можуть піддавати свою компанію кіберзагрозам.

Співробітників приваблює можливість працювати віддалено або зі свого пристрою в офісі. Безумовно, це зручно, але в той самий час може нести фінансові та репутаційні ризики для компанії.

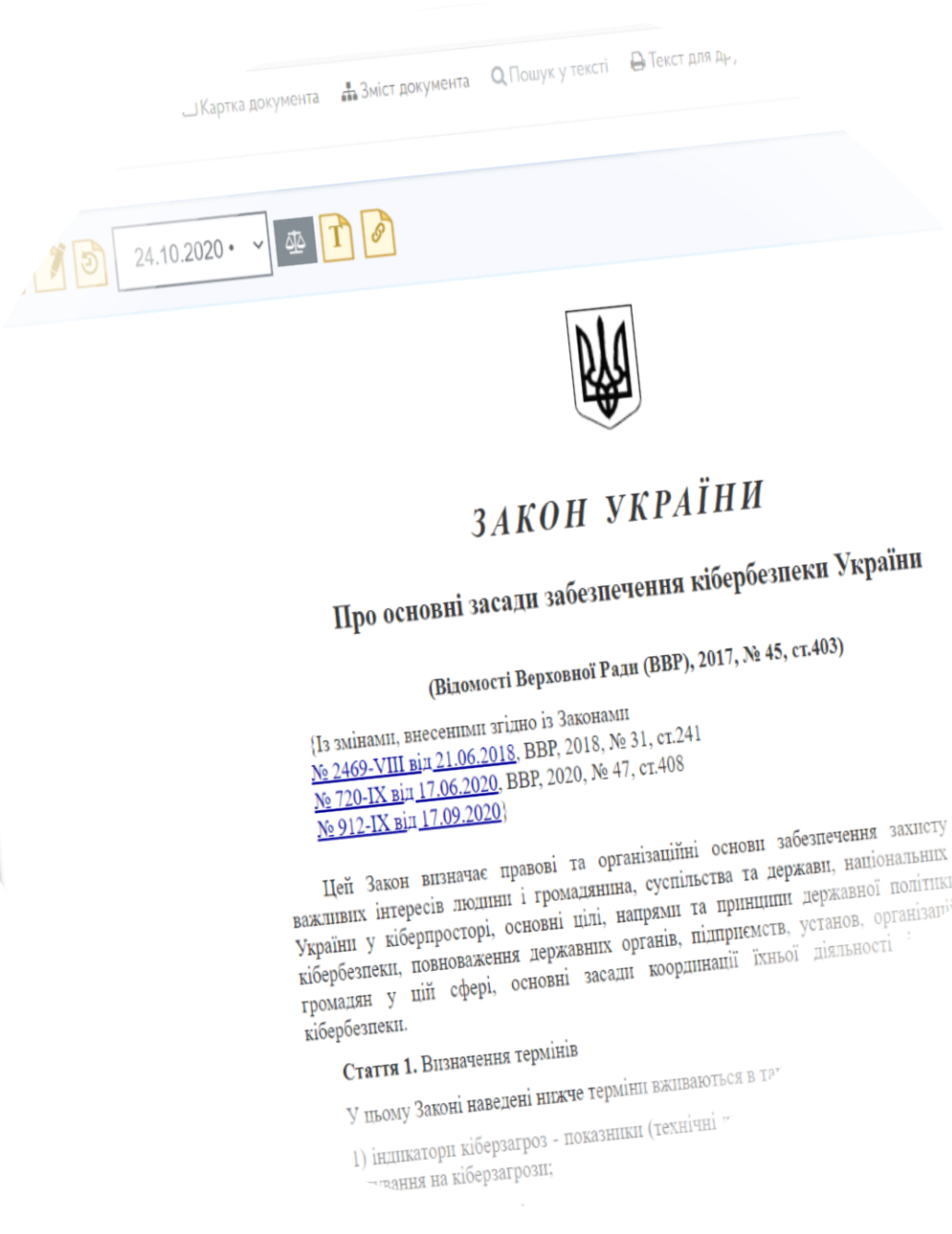
Через недостатньо захищений доступ до мережі пристрій може бути заражений вірусами, а важливі дані можуть пошкодитися або бути викраденими.

Тому усвідомлюючи всю серйозність проблеми, компанії все більше уваги приділяють можливостям штучного інтелекту забезпечувати кібербезпеку.



Поняття кібербезпеки

Законом України **"Про основні засади забезпечення кібербезпеки України"** визначаються основні поняття зазначеної проблемної галузі. Зокрема, Стаття 1 Закону визначає кібербезпеку 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».



Поняття кібербезпеки

Водночас Стаття 2 Закону пояснює: «1. Цей Закон не поширюється на: 1) відносини та послуги, пов’язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах; … 3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов’язані з функціонуванням таких мереж і ресурсів; …».

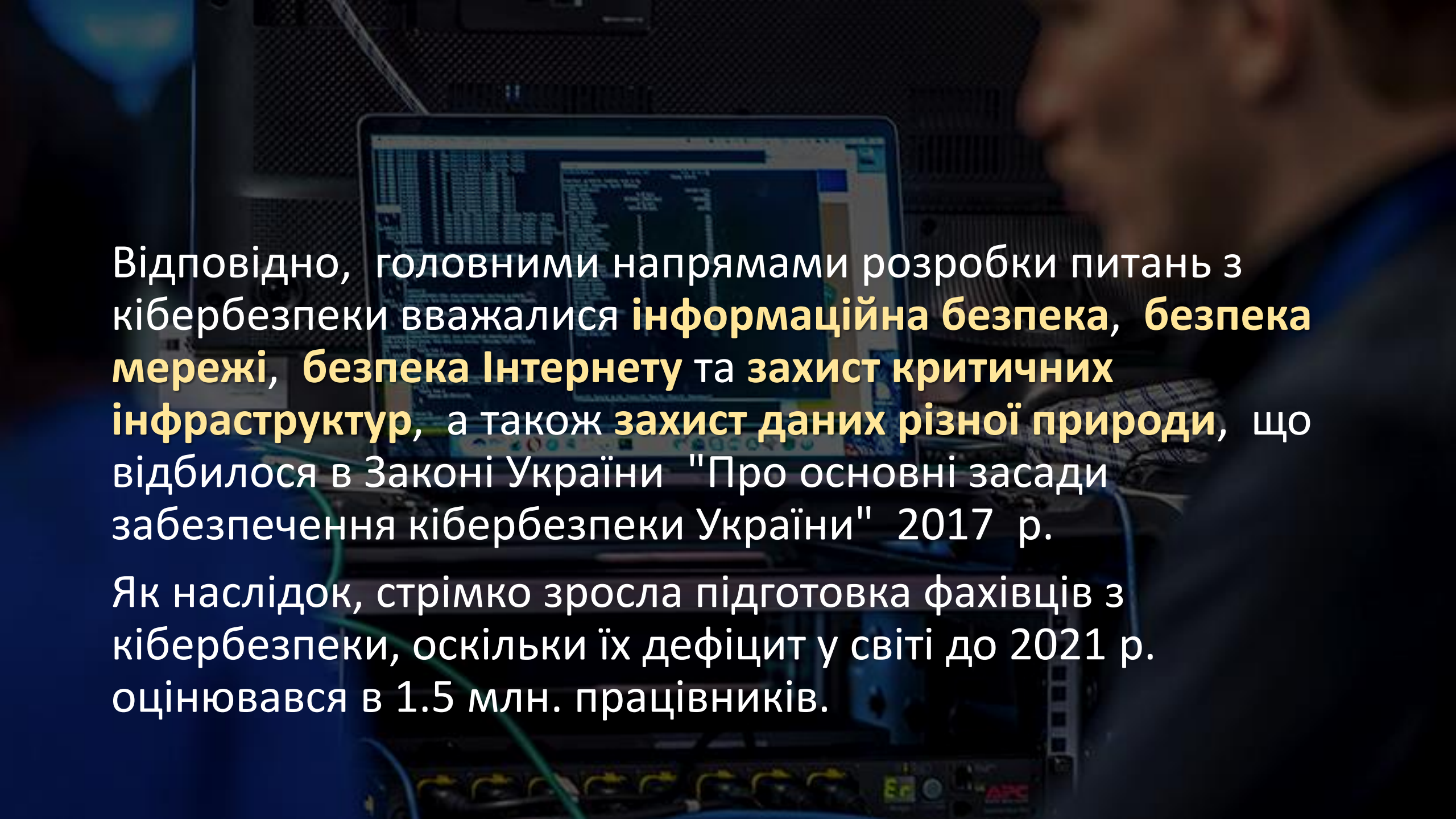
Інакше кажучи, чинний Закон не передбачає будь-які дії з безпеки стосовно людини, яка не входить до критичної інформаційної інфраструктури держави, а людський складник інтелектуального капіталу (який набуває зростаючого значення в усьому світі) не входить до критичного ресурсу України. І це в той час, коли в усьому світі основна боротьба йде за людські та інтелектуальні ресурси, тобто за тих, хто вже завтра буде забезпечувати конкурентоспроможність країни.

Із охопленням інформатизацією всіх сфер життя людини значення кібербезпеки вийшло на рівень компетентності з питань безпеки життєдіяльності людини і навіть перевищило його.

За даними 2017 Norton Cyber Security Insights Report, 978 млн. громадян країн G-20 у 2017 р. стали жертвами кіберзлочинності. З метою запобігання цьому явищу приймаються національні та регіональні програми, створюються міжнародні центри, приймаються програми спільної дії, затверджуються стандарти.

За оцінками світових експертів у 2016 р., світові витрати на кібербезпеку перевищували 70 млрд. дол. США на рік із щорічним зростанням на 10-15%. Зокрема, за даними експертів Gartner, Inc. зростання таких витрат у 2018 р. очікувалися в розмірі до 93 млрд. дол. США.

Програмними документами ООН визначалося, що **потрібна глобальна культура кібербезпеки**, яка буде вимагати від усіх учасників врахування наступних дев'яти взаємодоповнюючих елементів:



Відповідно, головними напрямами розробки питань з кібербезпеки вважалися **інформаційна безпека**, **безпека мережі**, **безпека Інтернету** та **захист критичних інфраструктур**, а також **захист даних різної природи**, що відбилося в Законі України "Про основні засади забезпечення кібербезпеки України" 2017 р.

Як наслідок, стрімко зросла підготовка фахівців з кібербезпеки, оскільки їх дефіцит у світі до 2021 р. оцінювався в 1.5 млн. працівників.

За 5 років після прийняття стандарту ISO почало суттєво змінюватись бачення проблеми кібербезпеки, оскільки людина дедалі більше перестає бути лише суб’єктом кіберзлочинів, перетворюючись на об’єкт сама по собі, а не тільки її фінансові та економічні інтереси та можливості. Так, за даними аналітичної компанії RAND Corporation, структура кібер-ризиків змінилася в останні роки. Усе більше аналітиків звертають увагу на те, що основні причини інцидентів в інтернет-ресурсах пов’язані з дією людського чинника, масовим зламом IoT-пристроїв та хмарних сервісів. Особливо ця проблема загострюється з посиленням цифрового гуманістичного характеру освіти, зростанням ролі соціальних мереж у житті людини в цілому та освіті зокрема, а також розумінням людства необхідності переходу до освіти протягом життя

Розглянемо друге питання:

Теоретико-методологічні питання кібербезпеки

Інформаційно-комунікаційні засоби як фундамент виникнення проблематики кібербезпеки

Сучасне життя все більше і більше будується навколо цифрових мереж, а соціальні медіа стають новим соціальним середовищем. Втручання в ці мережі створює реальну загрозу безпеці в галузі освіти та країни в цілому. Складники (чинники) мережі у спрощеному вигляді можна представити як (рис.1).

У якості вузла можуть виступати «агенти» мережі - люди (створювачі ресурсу та його контенту, адміністратори ресурсу, постійні або випадкові користувачі), технічні (термінальні станції, комп’ютери, приєднані до мережі гаджети, комунікатори) та інформаційні (бази даних, бази знань, керуючі системи тощо) засоби.

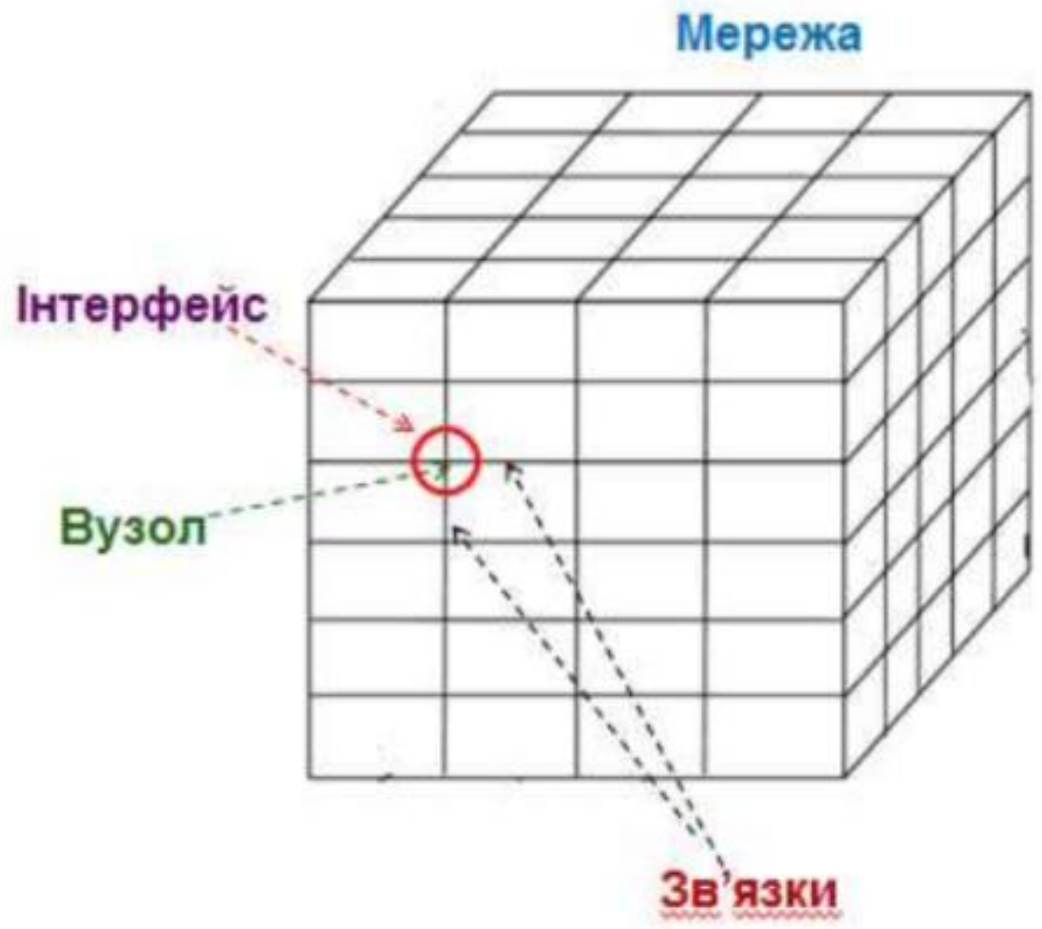


Рис. 1. Фрагмент мережі та її складники (чинники)

Усі агенти в залежності від їх природи мають притаманний їм інтерфейс і види зв’язку з іншими агентами.

Однак слід зауважити, що одночасно з розвитком технологій побудови мереж, їх ускладненням, використанням штучного інтелекту, появою хмарних і туманних технологій, зростанням потужності баз даних (БД) і баз знань (БЗ) мережа перестала бути просто посередником між користувачами (засобом комунікації).

Оскільки інформація в глобальній мережі існує поза окресленим простором і часом, сама мережа стає активним агентом впливу на людину, зберігаючи, насамперед, загальнодоступними великі обсяги даних. Будь-який користувач може увійти в мережу (легально або нелегально) та отримати доступ до необхідних вузлів (при використанні хмарних засобів конкретні вузли звичайному користувачу можуть бути невідомими), змінюючи також їх контент (наприклад, Wiki-об’єкт) за дозволеними правилами.

Проте інформація у БД та БЗ за дозволеними правилами може бути змінена або внесена з метою спотворення уявлення користувачів щодо даних, які вони шукають.

Певні користувачі мають змогу використовувати це для впливу на широку або цільову аудиторію, «спотворюючи» потрібні вузли (технічної або інформаційної природи) чи впливаючи на них засобами соціальної інженерії (якщо вузол – це людина).

Оскільки мережа є системою зв’язаних вузлів, то пошкоджений («спотворений») вузол може вплинути вже сам по собі на вторинні вузли. Окрім того, спотворена інформація починає існувати в мережі навіть незалежно від людини («агресора»), яка її ввела (рис.2).

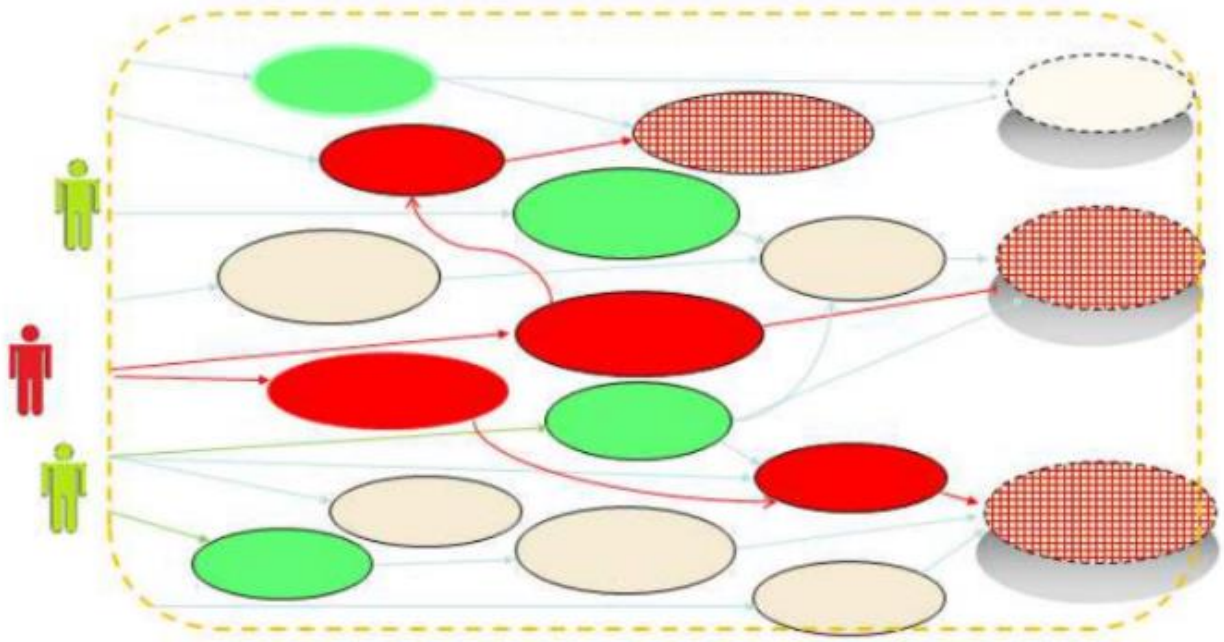


Рис. 2. Приклад активного фрагменту мережі та зовнішніх користувачів (зелений – звичайний, червоний – «агресор»).

У такий спосіб мережа набуває рис самостійного складника (чинника), що впливає на її властивості, функціонування та користувачів, а також систему «людина-техніка-середовище» (СЛТС) в цілому.

Усі чотири параметри дії мережі мають певні спільні критичні властивості з точки зору дієвості та впливу на користувача – ініціативність, ефективність, стійкість, гнучкість і продуктивність (табл.1).

Їх прояв щодо кожного чинника може бути охарактеризований певними показниками, характерними для відповідного параметру, а сукупність показників дозволяє оцінити загальний вплив чинника на мережу як СЛТС.

Таблиця 1

Складники мережі та їх властивості

Властивості	Вузол	Інтерфейс	Зв'язок	Мережа
Ініціатива	Усвідомлення інформації	Інформація щодо ситуації	Маршрутизація	Значення/мета
Ефективність	Продуктивність	Юзебіліті	Втрачені пакети	Якість сервісу
Стійкість	Відповідь на стрес	Послідовність	Надійність	Життєздатність
Гнучкість	Здатність до адаптації та змін	Режими відображення	Резервування	Реконфігурація
Продуктивність	Завантаженість	Перешкодостій-кість	Пропускна здатність	Щільність/ Складність

Загрози з боку кіберпростору

Спектр небезпек від відкритого кіберпростору постійно розширюється. Якщо десять років тому небезпеки для учнів шкіл можна було звести до відносно невеликої кількості груп – *вірусні атаки*, *кіберзлочинність*, небезпеки *інтернет-серфінгу*, – то на часі розмаїття небезпек і загроз зростає постійно, зачіпаючи всі можливі дії людини в мережі. Найбільшу загрозу мають приховані активні небезпеки.

Мережні загрози

Активне використання мереж, особливо дітьми та молоддю, супроводжується збільшенням різних видів загроз, що надходять з мережі. Особливо гостро ця проблема виникає при розробці та використанні соціальних мереж. Найбільш активні приховані загрози (для дітей), що походять з комп'ютерної мережі, можуть бути представлені наступною класифікацією:

Мережні загрози

- вірусні атаки,
- кіберзлочинність (спамерство, кардінг, фішинг, ботнети тощо),
- загрози від мережевого серфінгу (кібер-булінг, "дорослий" контент, незаконний вміст, насильство в режимі онлайн, розголошення приватної інформації, платні послуги тощо).

Типи загроз

Загрози, що надходять з мереж, можна розділити на наступні типи:

- активні та пасивні
- відкриті та приховані
- поточні та відкладені

Засоби кібербезпеки

У залежності від засобів дії, проблеми (і відповідні засоби) кібербезпеки можна класифікувати за такими групами (або рівнями):

- правові
- технічні
- інформаційні
- організаційні
- психологічні

Засоби кібербезпеки

У залежності від засобів дії, проблеми (і відповідні засоби) кібербезпеки можна класифікувати за такими групами (або рівнями):

- правові
- технічні
- інформаційні
- організаційні
- психологічні

Правовими та технічними питаннями кібербезпеки опікуються спеціалізовані фахівці та організації, тому вони не розглядаються на цьому занятті.

Засоби кібербезпеки

У залежності від засобів дії, проблеми (і відповідні засоби) кібербезпеки можна класифікувати за такими групами (або рівнями):

- правові
- технічні
- інформаційні
- організаційні
- психологічні

Інформаційні засоби можуть бути класифіковані залежно від завдань, що вирішуються користувачами:

- захист/засоби захисту,
- інформування,
- зміст,
- навчитися використовувати,
- безпека,
- життєстійкість,
- уникнення загроз.

Засоби кібербезпеки

У залежності від засобів дії, проблеми (і відповідні засоби) кібербезпеки можна класифікувати за такими групами (або рівнями):

- правові
- технічні
- інформаційні
- організаційні
- психологічні

Можливими цілями впливу кібербезпеки (крім об'єктів критичної інфраструктури) можуть бути:

– бази даних,
– персональні дані, серед яких фінансові,
– засоби масової інформації,
– соціальні мережі,
– освіта та професійна підготовка,
– підручники, історіографічні видання.

Засоби кібербезпеки

У залежності від засобів дії, проблеми (і відповідні засоби) кібербезпеки можна класифікувати за такими групами (або рівнями):

- правові
- технічні
- інформаційні
- організаційні
- психологічні

Організаційні засоби вирішення питань кібербезпеки:

– інформування,

– навчання культурі кібербезпеки, професійних працівників з кібербезпеки і населення в цілому,

– створення спеціальних засобів кібербезпеки,

– розповсюдження засобів кібербезпеки,

– контроль використання.

Засоби кібербезпеки

У залежності від засобів дії, проблеми (і відповідні засоби) кібербезпеки можна класифікувати за такими групами (або рівнями):

- правові
- технічні
- інформаційні
- організаційні
- психологічні

Психологічні засоби можна згрупувати в залежності від особистісного та міжособистісного рівня:

- національний,
- суспільний,
- груповий,
- індивідуальний,
- культурний,
- когнітивний,
- інтелектуальний та звички.

Засоби кібербезпеки

Хоча технологічні рішення розробляються у відповідь на кібератаки, зростає поінформованість про те, що роль людської діяльності та прийняття рішень у галузі кібербезпеки має вирішальне значення для підвищення ефективності відповідей на виникаючі загрози. Особливо це важливо з точки зору майбутньої робочої сили, оскільки молодь є особливо чутливою до зовнішнього впливу і є найбільш активною частиною "мережевого населення".

Людський чинник може бути системною слабшою ланкою, але водночас також може бути потужним ресурсом для виявлення та пом'якшення загроз, що виникають. Кілька областей найбільш критичних і невідкладних потреб та прогалин знань, що розглядаються в програмах кібер-досліджень країн НАТО та інших країн, можна визначити як такі: психосоціальні, культурні, концептуальні та організаційні аспекти

Соціальна інженерія та кібербезпека

Зміщення цілей кіберзлочинності з *технічних* (інформаційних) об'єктів на *людську ланку* спричинило появу **соціальної інженерії** як методів і технологій отримання необхідного доступу до інформації, заснованих на особливостях психології людей, зокрема - маніпуляція людськими страхами, зацікавленістю або довірою.

Основні типи соціальної інженерії

- Претекстінг
- Фішинг
- Троянський кінь
- Qui pro quo (послуга за послугу)
- Дорожнє яблуко
- Байтинг
- Зворотня соціальна інженерія
- Дружні листи
- Вішинг
- Контакти

Основні типи соціальної інженерії

Претекстінг — це набір дій, відпрацьованих за певним, заздалегідь складеним сценарієм, у результаті якого жертва може видати будь-яку інформацію або вчинити певну дію. Для використання цієї техніки зловмисник спочатку збирає певні дані про жертву (ім'я, місце навчання та проживання; дату народження; дані про батьків). Зловмисник спочатку використовує реальні запити з іменами щодо оточення жертви, а після того, як увійде в довіру, отримує необхідну йому інформацію або дії.

Основні типи соціальної інженерії

Фішинг — техніка інтернет-шахрайства, спрямована на отримання конфіденційної інформації користувачів авторизаційних даних різних систем. Основним видом фішингових атак є підроблений лист, відправлений жертві електронною поштою, який виглядає як офіційний. У листі міститься форма для введення персональних даних (пін-кодів, логіна і пароля тощо) або посилання на web-сторінку, де розташовується така форма.

Основні типи соціальної інженерії

Троянський кінь — це техніка ґрунтується на цікавості, страху або інших емоціях користувачів. Зловмисник відправляє лист жертві за допомогою електронної пошти, як додаток, до якого знаходиться «оновлення» антивірусу, ключ до грошового виграшу або компромат на співробітника. Насправді ж у вкладенні знаходиться шкідлива програма, яка після того, як користувач запустить її на своєму комп'ютері, буде використовуватися для збору або зміни інформації зловмисником.

Основні типи соціальної інженерії

Qui pro quo (послуга за послугу) — ця техніка передбачає звернення зловмисника до користувача по електронній пошті або корпоративному телефону. Зловмисник може представитися, наприклад, співробітником технічної підтримки та інформувати про виникнення технічних проблем на робочому місці та необхідність їх усунення. У процесі «вирішення» такої проблеми, зловмисник підштовхує жертву на вчинення дій, що дозволяють атакуючому виконати певні команди або встановити необхідне програмне забезпечення на комп'ютері жертви.

Основні типи соціальної інженерії

Дорожнє яблуко — цей метод є адаптацію троянського коня і полягає у використанні фізичних носіїв (CD, флеш-накопичувачів). Зловмисник зазвичай підкидає такий носій у загальнодоступних місцях. Для того, щоб виник інтерес до даного носія, зловмисник може нанести на носій логотип відомої популярної компанії.

Основні типи соціальної інженерії

Байтинг — метод, схожий на попередній, а також фішинг і троянський кінь, проте відрізняється тим, що байтер може запропонувати користувачеві реальну безкоштовну послугу (музику, фільм тощо) в обмін на конфіденційну (приватну) інформацію.

Основні типи соціальної інженерії

Зворотня соціальна інженерія — даний вид атаки спрямований на створення такої ситуації, при якій жертва змушена буде сама звернутися до зловмисника за «допомогою». Наприклад, створити оборотні неполадки в гаджеті жертви з попереднім інформуванням щодо служби “підтримки”. Користувач у такому випадку зателефонує або зв'яжеться по електронній пошті зі зловмисником сам, і в процесі «виправлення» проблеми зловмисник зможе отримати необхідні йому дані.

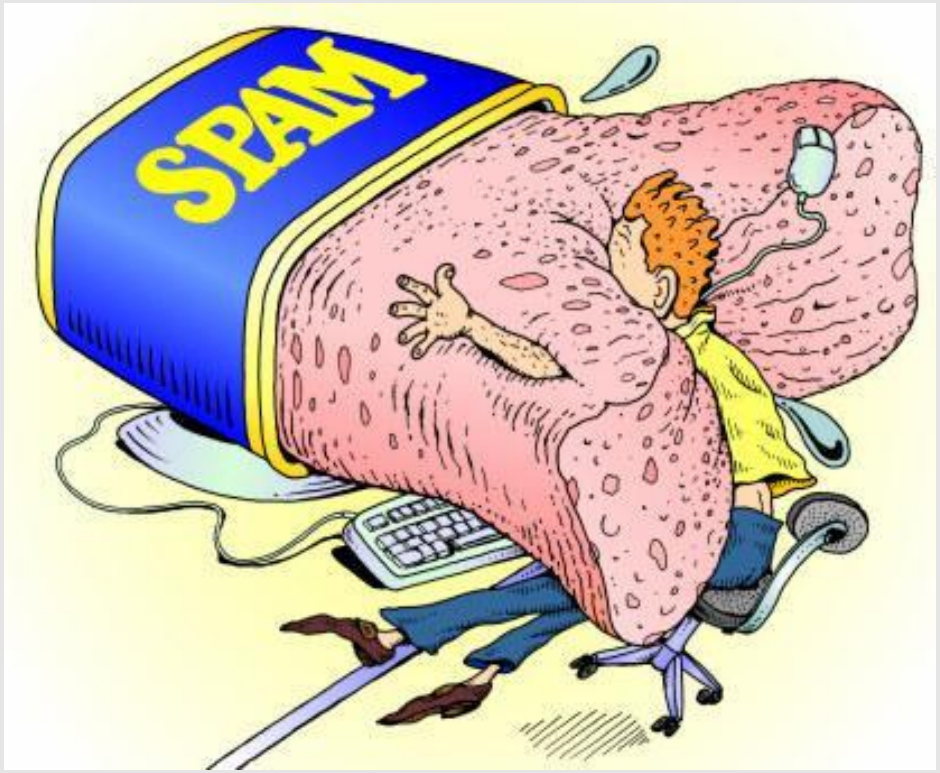
Основні типи соціальної інженерії

Дружні листи — надсилання електронних листів, у яких особу повідомляють про отримання спадщини, призів, бонусів чи дружнього переказу грошей.

Основні типи соціальної інженерії

Вішинг — голосова версія фішінгу. Як правило, дії пов'язані з телефонним шахрайством, метою якого є отримання реквізитів банківських карток або будь-якої іншої конфіденційної інформації або змушення жертви перевести гроші на банківський рахунок зловмисника.

Основні типи соціальної інженерії



Контакти — розсилання спаму від імені знайомих. Тобто, заволодівши чиїмось акаунтом, чи то в соціальній мережі, чи в електронній пошті, зловмисники можуть спробувати надсилати від його імені посилання. Психологічна дія, що побудована на схильності людини довіряти своїм знайомим і не дуже вагатися, коли отримують від них пропозицію відкрити посилання.

З огляду на положення Закону України “Про основні засади забезпечення кібербезпеки України” сфера освіти не входить до критичних галузей, на захист яких націлений цей Закон. Проте сьогоднішні учні та студенти в короткий термін можуть працювати в тих галузях. Тому вони вже сьогодні потребують захисту та відповідної підготовки, а також розуміння загальних можливих цільових груп кібербезпеки.

Бажаємо вам життя без спаму!