ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою

С.В. Легомінова, Ю.В. Щавінський, Т.М. Мужанова,
Ю.М. Якименко, Т.В. Капелюшна, Д.І. Рабчун

Професійна етика управлінської діяльності в кібербезпеці

Навчально-методичний посібник

Київ
2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою

С.В. Легомінова, Ю.В. Щавінський, Т.М. Мужанова,
Ю.М. Якименко, Т.В. Капелюшна, Д.І. Рабчун

ПРОФЕСІЙНА ЕТИКА УПРАВЛІНСЬКОЇ ДІЯЛЬНОСТІ В КІБЕРБЕЗПЕЦІ

Навчально-методичний посібник

Київ
2023

УДК 174:
ББК 87.7

Рекомендовано до друку
Вченою радою Державного університету телекомунікацій
(Протокол № __ від __._____.2023 року)

Укладачі: С.В. Легомінова, Ю.В. Щавінський,
Т.М. Мужанова, Ю.М. Якименко,
Т.В. Капелюшна, Д.І. Рабчун

Рецензенти:
Яковенко В.В., доктор технічних наук, старший науковий співробітник;
Терлецька Ю.М., кандидат психологічних наук, доцент;
Бударецький Ю.І., кандидат технічних наук, старший науковий співробітник.

ПРОФЕСІЙНА ЕТИКА УПРАВЛІНСЬКОЇ ДІЯЛЬНОСТІ В КІБЕРБЕЗПЕЦІ.

Навчальний посібник / С.В. Легомінова, Ю.В. Щавінський, Т.М. Мужанова, Ю.М. Якименко, Т.В. Капелюшна, Д.І. Рабчун, К. : ДУТ, 2023, 198 с.

Навчально-методичний посібник містить базові теоретичні знання, необхідні для забезпечення цілісного уявлення щодо розуміння проблем професійної та корпоративної етики в управлінні кібербезпекою, практичні завдання для закріплення навиків і умінь застосування етичних норм в управлінні кібербезпекою, які відповідають змісту навчальної дисципліни корпоративна та професійна етика в кібербезпеці.

Навчально-методичний посібник призначений для засвоєння базових понять на рівні новітніх досягнень в області професійної та корпоративної етики в сучасній інформаційній та соціокультурній діяльності, формування умінь застосовувати знання для аналізу, супроводу і контролю ефективної роботи колективу, вирішення проблем та впровадження заходів протидії кіберінцидентам відповідно до освітньої кваліфікації магістра з кібернетичної безпеки.

ЗМІСТ

ПЕРЕДМОВА

Особливістю сьогоднішнього глобального соціального процесу інформатизації суспільства є переважаюча діяльність людини у сфері суспільного виробництва зі збору, накопичення, продукування, обробки, зберігання, передачі та використання інформації. Цей процес разом із розвитком сучасних засобів мікропроцесорної та обчислювальної техніки призвів до створення кіберпростору з його позитивними і негативними сторонами.

Унікальні можливості кіберпростору, поряд із доступністю інформації, також дозволяють використовувати різні інструменти інформаційно-психологічного впливу на індивідуальну свідомість людини, колективну та масову свідомість суспільства. Основним інструментом цього впливу є інформація в різних її проявах. Її використання, позбавлене моральних критеріїв та цінностей, може бути небезпечним як для самої людини, так і для оточуючих, а в більш широких масштабах - і для суспільства загалом.

Тому, у зв'язку із необхідністю моніторингу інформації та її захисту, сформувався новий вид трудової діяльності – забезпечення безпеки інформації у кіберпросторі. Заснована на нових інформаційних технологіях і досягненнях науково-технічного прогресу, діяльність у кіберпросторі повинна ґрунтуватись не тільки на технічній ефективності але й на здорових моральних принципах, які забезпечать відповідність моральній системі суспільства. Система етичних знань і практичних рекомендацій, які орієнтовані на управлінську діяльність, є основою управлінської етики менеджера і повинна забезпечити підвищення ефективності виконання завдань трудової діяльності. Основними принципами сучасної управлінської етики є колективізм, соціальна справедливість, єдність слова і справи. Застосування етичних норм і принципів професійної етики фахівця кібербезпеки відіграє важливу роль у регулюванні трудової діяльності, пов'язаної з прагненням постійно вдосконалювати норми поведінки згідно з суспільними відносинами, що постійно змінюються.

Створення нових органів і підрозділів, які виконують завдання кібербезпеки, потребує застосування регламентації етичних норм у відносинах як всередині колективу так і між колективом і керівником, між колективом кібербезпеки та іншими колективами організацій. Така регламентація являє собою корпоративну етику, як систему колективних цінностей, традицій, переконань, норм поведінки співробітників окремої організації. Вимоги дотримання правил і норм поведінки в організації повинні бути встановлені у

етичних корпоративних кодексах, основна мета яких - згуртування колективу для ефективного досягнення необхідних результатів.

Забезпечення конфіденційності, цілісності доступності інформації в кіберпросторі разом із необхідністю забезпечення етичних норм професійної діяльності потребують засвоєння необхідних знань, умінь і навичок фахівців при виконанні ними функціональних обов'язків. Ефективне управління колективом кібербезпеки також потребує застосування етичних моральних норм при прийнятті управлінських рішень.

Тому важливою складовою підготовки сучасного фахівця з управління кібербезпекою є знання корпоративної та професійної етики, що регламентують поведінку, уміння і навички застосовувати етичні норми при виконанні функціональних обов'язків. Засвоєння цих знань умінь і навичок складають основу навчально-методичного посібника.

Метою навчально-методичного посібника є: висвітлення базових теоретичних знань, необхідних для забезпечення цілісного уявлення щодо розуміння проблем професійної та корпоративної етики в управлінні кібербезпекою; розвиток умінь та навичок застосування норм корпоративної та професійної етики в управлінні кібербезпекою;

Навчально-методичний посібник призначений для засвоєння базових понять на рівні новітніх досягнень в області професійної та корпоративної етики в сучасній інформаційній та соціокультурній діяльності відповідно до освітньої кваліфікації магістра з кібернетичної безпеки.

Вирішення визначених в навчально-методичному посібнику практичних завдань дозволить розвинути здібності застосування етичних норм при визначенні і розробці заходів інформаційної безпеки та оцінці ефективності управління інформаційними інцидентами і ризиками кібербезпеки, застосовувати етичні норми при обґрунтовуванні використання, впровадженні та аналізі кращих світових стандартів, практик з метою розв'язання складних задач професійної діяльності в галузі управління кібербезпекою.

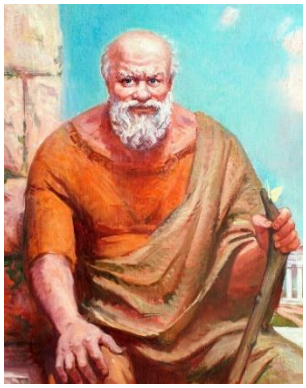
Розділ 1
ОСНОВИ ПРОФЕСІЙНОЇ ЕТИКИ

1.1. Предмет і завдання етики у сучасних умовах

Слово "етика[1]" виникло в Давній Греції і в різні часи мало різні значення. Спочатку воно означало місце перебування, спільне житло, потім - звичай, темперамент, характер, стиль мислення.

Ще у далекому 5 ст. до н. е. софісти[2] виявили, що закони природи не збігаються з проявами культури. Природна необхідність всюди однакова, а от звичаї і людські закони скрізь відрізняються. У зв'язку з цим гостро постала проблема порівняння різних звичаїв і законів, щоб з'ясувати, які з них кращі. Цікавий той факт, що як тільки люди взялися за процес зіставлення, відразу виявилося: численні звичаї і закони, які змінюються не тільки від народу до народу, але і з покоління в покоління, по-різному трактуються ще й в залежності від обґрунтування.

Пізніше етику почали розглядати як науку, що вивчає мораль, досліджує закономірності та принципи її виникнення, розвитку і функціонування, роль і призначення у житті окремої особистості та суспільства. Етика як наука виникла і розвивалася у межах філософії і розглядалася як практична філософія, або моральна філософія. Метою етики є раціональне обгрунтування моралі та виявлення її природи, сутності, місця і значення у розвитку людини і суспільства.



Засновником етики вважається давньогрецький філософ Сократ[3] якого вважають батьком античної етики [1].

Сократ в певному сенсі абсолютизував мораль, вважаючи її фундаментом гідного життя. Критикуючи софістів за відсутність позитивної програми, Сократ прагнув створити систему стійких загальних понять. Така вихідна установка не випадкова і конструктивна - в

[1] Е́тика (лат. ethica < дав.-гр. ήθική, утворене від грец. ήθος – «звичай», моральна психологія) – філософська наука, що вивчає мораль. Філософська дисципліна, яка вивчає мораль, суспільні норми поведінки, звичаї.
[2] Софісти – давньогрецькі мудреці 5-4 століть до н. е., які були мандрівними експертами з різних предметів, включаючи ораторське мистецтво, граматику, етику, літературу, математику, та елементарну фізику.
[3] Сокра́т (гр. Σωκράτης; МФА: [ˈsɒkrətiːz]; прибл. 470–399 до н. е.) – грецький філософ з Афін, який вважається засновником західної філософії та одним з перших філософів етичної традиції думки.

моральній діяльності слід керуватися знанням про моральність, не можна створити етику поза системою взаємопов'язаних понять. Для вирішення цієї задачі Сократ користувався спеціальним методом, в якому умовно можна виділити такі частини:

1) сумнів («Я знаю, що я нічого не знаю»);

2) іронія (виявлення протиріччя);

3) майевтика (подолання протиріччя);

4) індукція (звернення до емпіричного матеріалу, фактів);

5) дефініція (остаточне визначення шуканого поняття).

Доречно зазначити, що метод не втратив свого значення і в даний час, якщо використовувати його, наприклад, як спосіб ведення наукових дискусій.

Сократ започаткував евдемоністичні[4] традиції, стверджуючи, що сенс життя людини, вище благо - у досягненні щастя. Етика повинна сприяти усвідомленню та реалізації цієї установки. Щастя виражає зміст розсудливого, доброчесного буття, тобто лише моральна людина може бути щасливою (або розумною, що, по суті, те ж саме). Евдемоністична установка Сократа коригується його переконанням у самоцінності моралі: мораль не підпорядкована природному прагненню до щастя, а, навпаки, щастя залежить від моральності (доброчинності) людини. Відповідно до цього конкретизується завдання етики: допомогти людині стати моральною.

Складність реконструкції етичної позиції Сократа пов'язана з відсутністю його письмової спадщини, однак записи його висловлювань, зроблені учнями Ксенофонтом і Платоном, свідоцтва сучасників і, нарешті, особливості життя і смерті мислителя дозволяють судити про підстави його вчення. Факти біографії Сократа «мають силу етичних аргументів. Доля мислителя є зримим втіленням того людського ідеалу, який він теоретично обґрунтував» [1]. Сенс має тільки життя, згодне з переконаннями. Справжньою реалізацією переконань і, отже, сутності людини є вчинок, як найкращий спосіб самореалізації особистості, її моральна діяльність - ці та інші істини Сократ не тільки проголосив, він довів їх ціною власного життя.

Найбільш відомими дослідниками проблем етики в історії людства були Платон, Арістотель, Сенека, Марк Аврелій, Августин Блаженний, Б. Спіноза, І. Кант, А. Шопенгауер, Ф. Ніцше, А. Швейцер.

[4] Евдемонізм: 1) філософсько-етична традиція, за якою вищим або преферентним благом для людини є щастя; 2) моральний принцип, згідно з яким людина прагне до щастя

Учень Сократа Платон[5] продовжив роботу свого вчителя по дослідженню понять, результатом якої з'явився поділ світу на дві сфери [2]:

- світ чуттєвих речей (світ тіней);
- світ ідей (світ понять) – сфера безтілесних нечуттєвих форм, що є справжньою сутністю чуттєвих речей, що осягаються розумом.

Кожному класу предметів чуттєвого світу в безтілесному світі відповідає деякий "вид" чи "ідея" (справжнє буття речі). Чуттєві речі являють собою недосконалі копії ідей.

В області морального життя людини "світ ідей" – це ідеальний світ морального існування, це справжній світ, де "живе правда", описати цей світ можна тільки за допомогою моральних понять (справедливість, мудрість і т.д.). Це деякий зразок морального існування для смертних недосконалих речей. Головною пізнавальною і моральною задачею людини, змістом її існування є збагнення досконалості світу ідей, сходження до нього, на вершині якого може виявитися тільки мудрець, якому вдалося вийти за межі чуттєвого життя.

Вчення Платона можна розділити на:

- індивідуальну етику;
- соціальну етику (вчення про державу).

Етика Платона побудована, виходячи з його розуміння душі, тобто з усвідомлення вроджених чеснот, характерних для окремих суспільних станів. Якщо вони дотримуються, то у державі панує добро, що розуміється не як досягнення особистого щастя, а як досягнення суспільного благополуччя. Тому етика у Платона не індивідуальна, а соціальна, вона тісно зв'язана з політичною організацією суспільства. Це означає, що людина може бути моральною лише в правильно організованій державі. Взірець створеної держави і зразок створеної людини - така мета етичного і політичного вчення Платона.

Арістотель[6] позначав етику як особливу галузь практичної філософії, тому що вона намагається дати відповідь на питання: що нам робити? Сам мислитель вважав головною метою моральної поведінки щастя. Тоді під цим словом розуміли діяльність душі сповненою чеснотами або самореалізацію – розумні

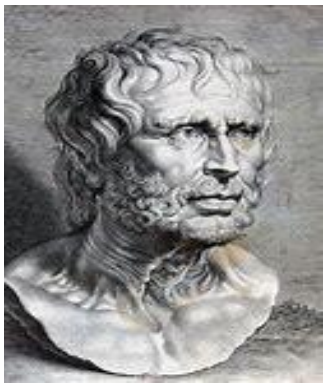
[5] Платóн (грец. Πλάτων; 427 до н. е. – 347 або 348 до н. е.) – давньогрецький мислитель, засновник філософської школи відомої як Академія Платона. Один з основоположників європейської філософії нарівні з Піфагором, Парменідом і Сократом.

[6] Арістóтель (дав.-гр. Ἀριστοτέλης; 384 до н. е., Стагіра – 322 до н. е., Халкіда) – давньогрецький науковець-енциклопедист, філософ і логік, засновник класичної (формальної) логіки.

діяння, далекі від крайнощів і дотримання золотої середини. Основними чеснотами вчення Арістотеля були розсудливість та поміркованість. Учень Платона був впевнений в тому, що предмет і основні завдання етики полягали не в самих знаннях, а у вчинках людей. І тут прозорою ниткою спостерігався нерозривний зв'язок між тим, у чому полягало благо, і тим, як його досягти. Початковим пунктом цієї науки є не принципи, а досвід суспільного життя. Ось чому тут не може бути та ж точність, яка властива, наприклад, математиці. Істину тут можна встановити лише в загальних рисах, приблизно [2].

Аристотель учив, що цілі бувають різні, утворюючи ієрархію. Повинна бути вища, кінцева мета, яку слід бажати саму по собі, а не розглядати як засіб для досягнення якоїсь іншої мети. Саме вона є вищим благом і може визначати міру досконалості особистості і соціальних інститутів. Вище благо – є щастя, для якого необхідні зовнішні блага, а також удача. Але в основній мірі воно буде залежати від духовної роботи – від діяльності, що співвідносить з чеснотою. І предмет вивчення і призначення етики як науки за Аристотелем – властивість душі діяти за зразком чеснот.

У трактаті "Про блаженне життя" Сенека[7] [3], як представник етики стоїцизму, проголошує, що "те життя щасливе, яке узгоджується з природою, а узгоджуватися з природою воно може лише тоді, коли людина володіє здоровим розумом, якщо дух її мужній і енергійний, благородний, витривалий і підготовлений до всяких обставин, якщо він, не впадаючи в тривожну недовірливість, піклується про задоволення своїх фізичних потреб, якщо він взагалі цікавиться матеріальними сторонами життя, не спокушаючись жодній з них, якщо він уміє користуватися дарами долі, не стаючи їх рабом" (Луцій Анней Сенека. Про щасливе життя). Дотримуючись доктрини стоїків, Сенека вважає, що все складається з матерії й Бога. В основі природи лежить Логос – розум, розлитий у всьому сущому, який забезпечує бездушним предметам «стійкий стан», рослинам – «проростання», тваринам – «саморух», а в людях і Богах виступає як розум у власному сенсі.



[7] Сенéка Аннéй Лýцій (лат. Lucius Annaeus Sĕnĕca minor; Сенека молодший) (4 до н. е. – 19 квітня 65) – давньоримський філософ, поет, державний діяч і оратор, консул-суффект 55 року. Син філософа Сенеки Старшого.

Етика Сенеки - етика пасивного героїзму [4]. Змінити в житті, по суті, нічого не можна. Можна тільки зневажати її напасті. Найбільша справа в житті – твердо стояти проти ударів долі. Але ж це означає, що доля активна, а людина пасивна. Він займає лише оборонну позицію. Потрібно панувати над своїми пристрастями, не бути у них в рабстві. Що ж до щастя, то воно цілком залежить від нас в тому сенсі, що нещасливий лише той, хто сам вважає себе нещасним: "Кожен нещасний настільки, наскільки вважає себе нещасним".

Марк Аврелій[8] також, як і всі стоїки того часу, зацікавлений в обґрунтуванні автономії морального вибору. Чеснота повинна підкорятися іншій причинності, ніж природні явища: яку б картину світу не вибрала людина – стоїчну, атомістичну і т. п., – вона повинна зробити себе гідною божественній допомозі. У центрі його антиматеріалістичних вчень стоїть часткове володіння людиною своїм тілом, душею і духом, носієм яких є благочестива, мужня і керована розумом особистість – володарка (тільки над духом), вихователь почуття обов'язку і обитель совісті [1].

Основою етики Спінози[9] служить проповідування ідея про те, що воля або здатність психічної діяльності істотно не відрізняється від розуму [1]. Вона (воля) не що інше, як прагнення розуму утримувати ідеї, які йому приємні і звільнитися від тих, які йому неприємні. Бажання – це ідея, яка стверджує або заперечує себе. Етика, доведена в геометричному порядку (лат. Ethica, ordine geometrico demonstrata), загальновідома, як Етика, філософський трактат латинською мовою, написаний Бенедиктом Спінозою в період між 1661 та 1675 роками. Книга була вперше опублікований в 1677 році після смерті автора.

[8] Божественний Марк Авре́лій Антони́н (лат. Marcus Aurelius Antoninus Augustus; 26 квітня 121, Рим – 17 березня 180, Віндобона, нині Відень) – римський імператор з 169 року, належав до династії Антонінів. Був сином Анія Вера і Доміції Луцілли. Відомий як філософ-стоїк.

[9] Бенеди́кт Спіно́за (справжнє ім'я Бару́х; івр. שפינוזה ברוך, лат. Benedictus de Spinoza; 24 листопада 1632, Амстердам – 21 лютого 1677, Гаага) – нідерландський філософ єврейського походження, науковець, політичний та релігійний мислитель, біблійний екзегет і критик. Розвинув учення про єдину нескінченну субстанцію, що є причиною самої себе (принцип causa sui), з безмежною кількістю атрибутів, з-поміж яких людям відомі лише два: протяжність і мислення.

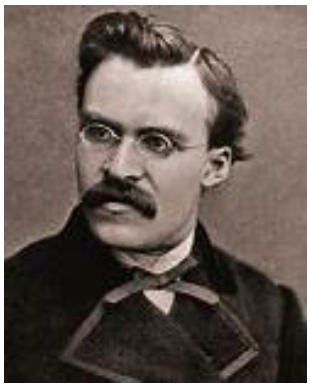
Ця праця, мабуть, найбільш амбіційна спроба застосування Евклідової геометрії[10] в філософії. Спіноза ставив на початку кожного розділу невелику кількість понять та аксіом з яких він намагався вивести сотні висловлювань та тверджень, таких як «коли розум уявляє нестачу власної сили мислення, то пригнічується цією думкою», "Вільна людина ні про що не думає менше, ніж про смерть ", та «Людський розум не може бути повністю знищений тілом, та деякі наслідки цих спроб залишаються навічно». Згідно Спінозі, в пристрасті людина – істота стражденна, тобто обмежена, безсила, раб речей. Вона може звільнитися і стати діяльною тільки через розум. Зрозуміти світ, значить стати вільним від нього. Оскільки свобода тільки в думках, то наше розуміння речей є міра нашої етики, моральності. Моральним, етичним є те, що розвиває розум; аморально те, що затьмарює або обмежує його [5].

Етика Шопенгауера[11] [1] ґрунтується на положенні про те, що в боротьбі світових сил повинно виразно відчуватися прагнення першооснови всього буття – волі – повернутися до свого істинного, несвідомого буття. Це прагнення виражається на тлі скорботи, болю і страждань, які панують у житті. На думку Шопенгауера, справжнім змістом життя є постійна боротьба волі, у якій вона, нудячись, прагне до спокою свого несвідомого буття. Світ, як арена цієї боротьби, не кращий, а найгірший з усіх світів. Потяг волі повернутися до свого загального буття найбільше виявляється, згідно Шопенгауеру, у двох явищах: в процесі розмноження, в якому індивід прагне відтворити рід; і у співчутті, джерелі моралі, де індивід серед подібних йому усвідомлює себе представником людського роду. Чим більше особа цурається своєї індивідуальності і підноситься до загального, тим більше вона звільняється від життєвих страждань – це основний пункт етики Шопенгауера.

[10] Евкли́дова геоме́трія – геометрична теорія, заснована на системі аксіом, вперше викладеній у підручнику «Начала» Евкліда (дав.-гр. Στοιχεῖα Stoicheia, III століття до н. е.). Метод Евкліда полягає в прийнятті невеликого набору інтуїтивно зрозумілих аксіом і виведення з них багатьох інших теорем.

[11] А́ртур Шопенга́уер (іноді також зустрічається – Шопенга́вер)([ˈʃoʊpənhaʊ.ər] SHOH-pən-how-ər; Німецька: [ˈaɐ̯tʊɐ̯ ˈʃoːpn̩haʊ̯ɐ]; 22 лютого 1788 – 21 вересня 1860) – німецький філософ-ірраціоналіст, відомий своїм вченням про безособову несвідому світову Волю та песимізмом.

Поділяючи погляди А. Шопенгауера, Ф.-В. Ніцше[12], категорично виступив проти сучасної йому європейської моралі (не тільки проти моральності, реальних моральних стосунків, які завжди недосконалі, а й проти моралі як системи норм бажаних моральних стосунків людей), за "переоцінку цінностей", насамперед моральних (етика самовиправдання). "Необхідно знищити мораль, щоб звільнити життя", – стверджував філософ. Етиці як науці про мораль, на його думку, не вистачає проблеми самої моралі: "...сама цінність цих цінностей повинна бути колись поставлена під сумнів..." [6]. Різновиди моралі, за твердженнями Ф.-В. Ніцше, загалом належать або до моралі аристократів (кращих), або до моралі рабів (гірших).

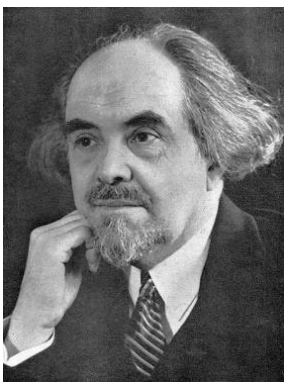


Мораль аристократів – це "мораль переваги", одвічна, природна, самодостатня. Вона "виростає із торжествуючого самоствердження" людини як неприборкана сила природи.

Мораль рабів, на думку мислителя, сформувалася під впливом античної філософи та християнської релігії і втілилась у численних аскетичних церковно-доброчинних, соціалістичних та інших концепціях людської солідарності. В Європі, за його переконаннями, панує мораль рабів, яку вважають єдино можливою мораллю, мораллю загалом.

Етикою займалися всі великі вітчизняні мислителі: св. Тихон Задонський, св. Феофан Затворник, В.С. Соловйов, М.О. Бердяев.

Микола Олександрович Бердяев[13] виділяв три рівні моральності:



- перший рівень моральності – це творчість і стать, чоловіче та жіноче, рід та особистість;
- другим рівнем моральності є творчість та любов, шлюб та сім’я;
- третім рівнем моральності є творчість та мораль, нова етика.

[12] Фрі́дріх Ві́льгельм Ні́цше (нім. Friedrich Wilhelm Nietzsche, МФА: [ˈfʁiːdʁɪç ˈvɪlhəlm ˈniːtʃə]; 15 жовтня 1844, село Рекен, (нині район Бургенланд земля Саксонія-Ангальт), Королівство Пруссія, Німецький союз – 25 серпня 1900, Веймар (нині земля Тюрингія), Німецька імперія) – німецький філософ, психолог і класичний філолог, представник ірраціоналізму.

[13] Мико́ла Олекса́ндрович Бердя́єв (родився 6 (18) березня 1874, маєток Обухів, під Києвом) релігійний філософ українського походження. Його вважають одним із найвидатніших філософів XX сторіччя. Є автором близько 40 книг, зокрема: «Зміст творчості», «Філософія вільного духу».

На першому рівні моральності Микола Олександрович описує, що для нашої епохи істотно характерним є осмислення проблеми статі та глибока потреба розуміння статевої стихії. Другий рівень моральності за Бердяєвим характеризується тим, що існує три стани статі: підзаконної сім'ї, аскетизму та розпусти. На третьому рівні моральності автор розповідає про мораль в суспільстві, як мораль виявлялася раніше і яке зараз вона займає місце у суспільстві. Багато людей вважають, що закони являються мораллю, але все ж таки закони є закони, а мораль це свідоме ставлення до певних виявів особистості в суспільстві, або поведінки людей в ньому.

Сучасна етика – теорія моральних відносин, що визначається умовами розвитку постіндустріального суспільства. Її головними цілями є обґрунтування моделі суспільного життя, заснованої на принципах справедливості в рамках інформаційної цивілізації, гуманізація всієї системи суспільних відносин на засадах самореалізації особистості. У суспільстві, заснованому на принципах справедливості, зростає роль сфери моралі і затверджуються її нові види:

1) етика ненасильства;

2) екологічна етика;

3) біоетика;

4) інформаційна етика.

Особливістю *сучасної моралі* є зрощування професійних знань і навичок працівника з моральними якостями його особистості. Професійні рішення вимагають від особистості прийняття моральних зобов'язань. У сучасному суспільстві традиційні моральні цінності поєднуються з правилами діяльності товариства, а поняття добра, зла, совісті, справедливості та відповідальності повинні відповідати зростанню рівня духовної культури, досягненням наукових знань і технологічному прогресу відтворення. Сучасна моральна людина повинна бути скромною, гуманною, відповідальною і водночас діловитою, непримиренно ставитися до подвійної моралі, мати самовладання і витримку і дорожити довірою людей.

Мораль сучасного інформаційного суспільства повинна бути орієнтована на такі цінності:

1) благородство цілей, ідеалів і установок;

2) гуманізм і прогрес;

3) наукові обгрунтування і наявність трудової основи.

Сучасна мораль відображає реальні суспільні і людські протиріччя. Вони можуть бути вирішені, якщо будуть ґрунтуватися на духовних засадах, вимозі від кожного слідувати моральним потребам, нетерпимості до проявів аморальності. Тому ознаками морального прогресу сучасного українського суспільства слід вважати:

1) зростання духовної свободи особистості і розширення можливостей її вдосконалення;

2) посилення впливу моралі на всі сфери суспільного життя;

3) подолання конфліктів шляхом застосування моральних способів впливу;

4) підвищення рівня морального протесту проти бездуховності і аморальності;

5) теоретичний розвиток моралі і постійне збагачення етики як науки;

6) визначення більш досконалих способів впливу на моральну поведінку людей.

Підставою для твердження про моральний прогрес суспільства є рівень свідомості і відповідальності кожної людини. Мораль розвивається на зближенні належного і сущого, формуванні норм та ідеалів, які відповідають вимогам інформаційної цивілізації.

Структура етики, як науки, включає сьогодні шість змістових блоків:

- емпірична етика;
- загальна теорія моралі;
- нормативна етика;
- педагогічна етика;
- професійна етика;
- історія етичної думки.

Можна говорити про "етику вченого" або "медичну етику", маючи на увазі певні принципи поведінки вченого, лікаря або засуджувати ті чи інші вчинки за "неетичність".

Етика, як наука, досліджує свій *предмет* з конкретно-історичних, філософсько-світоглядних позицій у тісному взаємозв'язку з соціальними відносинами. Вона розкриває закони виникнення й історичного розвитку моралі, її сучасний стан і функції, аналізує соціальну сутність моральності, обґрунтовує її історичну прогресивність.

Етика розглядає людину в цілісності, єдності всіх її складових. Методологічне значення етичного пізнання полягає в тому, що воно має як

евристичний[14] аспект, який пов'язаний насамперед з досягненням нових знань, так і оціночний, який передбачає розкриття ціннісного змісту моральності.

Етика, вивчаючи *предмет* в його соціальній обумовленості з усім суспільним життям, науково обґрунтовує етичні категорії, принципи і норми, проводить їх філософський і соціальний аналіз. Узагальнюючи якісно нові моральні відносини в суспільстві, вона уточнює, розширює свій предмет дослідження, вивчає загальні закономірності моральної свідомості, визначає роль об'єктивного і суб'єктивного факторів у формуванні моралі, відкриває те нове, що вносить життя у її зміст, виявляє якими мотивами керуються люди, вчиняючи певним чином, чи можна взагалі піддавати людські вчинки моральній оцінці і який у такому випадку їх об'єктивний критерій.

Таким чином, *об'єктом дослідження етики виступає мораль. Предметом етики є* ***моральні норми, правила, принципи, уявлення, поняття тощо.***

Сучасна етика - це галузь знань, що стрімко розвивається і надзвичайно популярна в гуманітарній науці. Можна без перебільшення сказати, що етична тематика і її наслідки для соціальної теорії стали головною інтелектуальною лінією в сучасній західній філософії. Ця ситуація в літературі отримала назву "*Етичний поворот*". Але, крім глибоких теоретичних міркувань, сучасна етика відрізняється однією суттєвою рисою: вона стала принципово проблемною. Вона обертається навколо найбільш складних, конфліктних ситуацій нашого життя, супроводжуючих повсякденне існування людини.

Звідси виникають три великі галузі сучасної етичної теорії: професійна, корпоративна та прикладна етика.

Одним з головних *завдань* етики є правильне формування та правильне усвідомлення понять «*мораль*» та «*моральність*». Головне завдання моралі формувати у людей правильні моральні цінності.

Тому науковці виділяють декілька опосередкованих завдань, які повинна виконувати етика, як наука:

- вивчення історії виникнення моралі;
- визначити причин, які послугували виникнення такого поняття, як «мораль» та «моральні цінності»;
- дати загальне поняття моральним цінностям;
- формування понять «щастя», «нещастя»;

[14] Еври́стика (грец. ευρίσκω (heuristiko) – знаходжу, відшукую, відкриваю) – наука, яка вивчає творчу діяльність, методи, які використовуються у відкритті нового і в навчанні.

- зафіксувати в свідомості людини правильні моральні якості;
- формування понять добра і зла;
- виховне завдання.

В наші дні етика, як знання і як практика, що бажає встановити найбільш правильні стосунки між людьми, діє в трьох великих вимірах:

- в умовах професійного співтовариства;
- в умовах спільної діяльності людей різних професій і статусів;
- в ситуації публічного обговорення найбільш гострих моральних дилем суспільної практики, що виникають як конфлікт перших двох способів існування з моральною гідністю людини.

Теорію сучасної етики та застосування її принципів у кібербезпеці сьогодні вивчають у вищих навчальних закладах. Предметом вивчення навчальної дисципліни "Корпоративна та професійна етика в кібербезпеці" є: систематизовані норми, принципи поведінки та механізми вирішення складних етичних ситуацій при управлінні інформаційною та кібернетичною безпекою.

Завдання навчальної дисципліни:

- засвоєння базових понять на рівні новітніх досягнень в області професійної та корпоративної етики;
- розвиток умінь та навичок застосування норм корпоративної та професійної етики в управлінні інформаційною безпекою та кібербезпекою при визначенні і розробці заходів інформаційної безпеки та оцінці ефективності управління інформаційними інцидентами і ризиками;
- формування навичок в організації управління інформаційними інцидентами і ризиками інформаційної безпеки.

Відтак, *завдання* етики полягає в адаптації людини протягом її життя до швидких і кардинальних змін цивілізації, що виражається у трьох напрямах: звільнити свідомість від зайвих пережитків і непотрібних обмежень; виокремити, обґрунтувати і закріпити моральні цінності, необхідні для нормального існування і розвитку людства; створити шляхи впровадження в життя зазначених вище цінностей.

Питання для самоконтролю:

1. В чому суть спеціального методу Сократа створення стійких загальних понять?

2. В чому полягає особливість етичних поглядів Платона, Арістотеля?
3. Хто є представником етики стоїцизму?
4. Що є об’єктом і предметом дослідження етики, як науки?
5. Які особливості сучасної етики?
6. Які завдання виконує етика, як наука?
7. Чим може допомогти знання етики фахівцям кібербезпеки?

Завдання:

1. Порівняти звичаї українців і поляків.
2. Зробити аналіз етичних поглядів св. Тихон Задонського та св. Феофана Затворника.

1.2. Роль професійної та корпоративної етики у становленні професіоналізму

Професіоналізм відображається в знаннях, вміннях та відповідальному ставленні до виконання професійних обов'язків. Розвиток професіоналізму вимагає від працівників високої моральної дисципліни та відповідального ставлення до своєї роботи. Однією з важливих складових професіоналізму є професійна та корпоративна етика, яка впливає на розвиток і зміцнення професійних якостей. Дослідники [1, 6-11] відзначають, що професійна етика - найдавніша з усіх трьох напрямків. Традиційно вважається, що перший звід саме професійних правил склав давньогрецький лікар Гіппократ[15], з яким пов'язане виділення медицини в окрему науку. Заради справедливості слід зауважити, що не він сформулював клятву лікаря, а скоріше узагальнив різні обітниці, які давалися грецькими жерцями бога лікування Асклепія[16]. Ця клятва стала прообразом численних кодексів лікарів, існуючих у різних країнах. Далі історія

[15] Гіппокра́т з Ко́су (грец. Ιπποκράτης; близько 460 до н. е. – бл. 370 до н. е.) – грецький лікар золотої доби Афін (Класична Греція), який вважається однією з найвизначніших осіб в історії медицини. Він відокремив медицину як дисципліну від релігії, стверджуючи та переконуючи, що хвороба не є покаранням, божою карою, але радше продуктом зовнішніх чинників, дієти та шкідливих звичок. Йому приписують авторство «Клятви Гіпократа».

[16] Аскле́пій (від грец. Ασκληπιός, також Ескулап від лат. Aesculapius) – давньогрецький бог лікування, син Аполлона й Короніди, доньки владаря лапітів Флегія. Мистецтва лікування навчився від кентавра Хірона, міг навіть воскрешати мертвих. Зевс убив Асклепія блискавкою за те, що він повернув до життя мертвого, тим самим порушивши встановлений богами порядок.

професійної етики простежується в якості об'єднавчих документів, статутів і клятв різних корпорацій.

У Середні віки звертають на себе увагу статути і кодекси ремісничих цехів,

монаших спільнот, а також лицарських орденів. Останні, можливо, найпоказовіші в цьому плані, оскільки підкреслюють виключну, божественну значимість свого служіння. Не випадково авторство статуту і присяги найпершого лицарського ордену тамплієрів[17] (1118) належить знаменитому середньовічному філософу Бернарду Клервоському[18] (1091-1153).

Однак масове поширення кодексів професійної етики почалося з другої половини XX ст., коли професіоналізм став вважатися однією з найвищих цінностей соціальної практики.

У чому полягають найважливіші риси професійної етики?

По-перше, вона виражена у вигляді вимог, звернених до представників конкретної професії. Звідси випливає її нормативний образ, закріплений у вигляді красиво сформульованих кодексів-декларацій. Як правило, вони представляють собою невеликі за обсягом документи, що містять у собі заклик відповідати високому покликанню професії. Поява даних документів свідчить про те, що носії професії стали усвідомлювати себе в якості єдиного співтовариства, що переслідує певні цілі і відповідає високим соціальним стандартам.

По-друге, документи з професійної етики наповнені переконанням у тому, що цінності, нею сповідувані, цілком очевидні і слідують з простого аналізу діяльності найбільш яскравих представників даного роду діяльності. По-іншому не може бути, бо самі кодекси витримані в стилі послання людям, яким надана велика честь займатися значущим суспільним служінням. Звідси випливають принципи відповідальності, об'єктивності, високої компетентності, відкритості до критики, доброзичливості, людинолюбства, небайдужості, необхідність постійного вдосконалення професійної майстерності. Ніде не дається розшифровка цих цінностей, бо вважається, що вони інтуїтивно зрозумілі

[17] Тампліє́ри – у 1119–1312 роках католицький чернечо-лицарський орден. Заснований у Єрусалимському королівстві після Першого хрестового походу (1096) для гарантування безпеки великої кількості паломників із Європи, що йшли до Єрусалима.

[18] Берна́рд Клерво́ський (лат. Bernardus abbas Clarae Vallis, фр. Bernard de Clairvaux, 1090 – 20 серпня 1153) – французький монах-цистеріанець. Засновник і перший абат Клервоського монастиря. Реформував Орден. Вважався «голосом сумління» та домінантною фігурою у західному християнстві свого часу.

кожному члену суспільства. Крім цього, завжди можна відшукати посилання на те, що є професійним злом і ніяк не може бути терпимим з погляду зазначених цінностей. Наприклад, відмова в наданні допомоги, використання службового становища, недотримання професійної таємниці, підміна компетентності особистою думкою і т.д.

Є ще одна важлива особливість професійного розуміння моралі. Цей стиль етики надає найвищий статус регульованій нею діяльності. Професія, чиї цінності вона покликана захищати – лікаря, вченого, педагога, юриста, – рахується самою високою з усіх існуючих, а її представники – елітою суспільства. Так, у вже згадуваних численних кодексах поведінки лікарів простежується думка, що вони покликані не тільки боротися зі смертю, але й знають секрети здорового способу життя. У деяких особливо радикальних випадках професія визнається еталоном моральності, бо відповідає зразку жертовності, самовідданості і сприяє процвітанню суспільства.

Наступна особливість професійної етики стосується проблеми характеру регулювання діяльності та авторитету, що стоїть за ним. Зрозуміло, що авторитетом вважається само професійне співтовариство, а виступати від його імені можуть найбільш шановані представники, яким надано високу довіру. З даного контексту стає очевидно, що і розслідування, і санкції – також справа самого співтовариства. Його моральний суд і вирок – це рішення колегії професіоналів щодо тих, хто неправильно зрозумів своє високе призначення, вжив свій статус на шкоду спільноті і тим сам себе викреслив з неї. Виходячи із зазначених установок, неможливо уявити, щоб етичний контроль здійснювався сторонніми спостерігачами. Як відомо, професійне середовище вкрай болісно ставиться до всяких форм зовнішнього регулювання.

Характер санкцій, передбачених професійною етикою, також випливає з уявлень про особливий статус даного виду діяльності. Якщо людина займає настільки високе положення в суспільстві, то і вимоги до нього повинні бути найвищими. Практично жоден кодекс професійної етики не обходиться без вказівки санкцій, що застосовуються до порушників. Професія пишається своєю соціальною значимістю, тому готова виключати зі своєї сфери відступників. Як правило, санкції ранжовані: від оголошення зауваження від імені колегії уповноважених осіб до позбавлення професійного статусу. Обов'язково в розділі санкцій згадано про інші заходи впливу, крім етичних, – законодавчі або адміністративні. Тим самим зайвий раз підкреслюється соціальна роль професії

і зацікавленість самого суспільства в її розвитку. Відповідно, в кодексах обов'язково міститься перерахування можливих порушень. І так само, як у випадку з основними ціннісними орієнтирами професіоналізму, їх сенс повинен бути інтуїтивно зрозумілим представнику кожного конкретного роду занять.

Професійна та корпоративна етика є важливими складовими успішної роботи в будь-якій професії. Професійна етика описує етичні норми та стандарти поведінки, що регулюють взаємини між працівниками та їх клієнтами, а також ставлення до ділової етики та етики взаємин з партнерами. Корпоративна етика відображає етичні норми, які регулюють внутрішні взаємини в організації та ставлення до корпоративної культури та цінностей.

Виходячи з усього сказаного, стають очевидними завдання професійної етики. Для співтовариства, що стоїть за нею, важливо не втратити свій статус, довести суспільну значимість, відповісти на виклики швидкомінливих умов, зміцнити власну згуртованість, виробити загальні стандарти спільної діяльності і захистити себе від домагань інших сфер професійної компетенції. У цьому зв'язку варто зауважити, що в наші дні найбільшою активністю в даній сфері володіють в основному молоді професії, яким дуже важливо довести своє право на існування.

Проте даний вид етичної теорії і практики володіє деякими недоліками. З першого ж погляду можна відзначити її закритий, вузький характер, де надія покладається лише на власний авторитет при здійсненні моральної оцінки, що обертається необґрунтованими амбіціями при вирішенні гострих конфліктних ситуацій. Професійне середовище – стихія принципово консервативна, традиції і засади відіграють у ній величезну роль. Це добре, коли мова йде про спадкоємність і розвиток, наприклад наукових шкіл, але чи достатньо в сучасному світі будувати етичне регулювання тільки на традиціях і підвалинах? Крім того, моральна свідомість не може погодитися з тим, що головною цінністю будь-якої соціальної практики вважається професіоналізм. Якщо вже у сфері конкретної діяльності виникла необхідність обговорювати моральні проблеми, це означає, що звичайних уявлень про професійний обов'язок недостатньо для її нормального функціонування. Співвідношення професіоналізму та моральності – одна з найпопулярніших тем у філософії XX ст.

Підсумком роздумів філософів можна визнати те, що у порівнянні з вічними моральними цінностями суть професіоналізму не можна визнати очевидною і незмінною.

У деяких посібниках з сучасної етики поняття «професійна етика» і «корпоративна етика» використовуються як синоніми. Це не зовсім вірно. Звичайно, співтовариство професіоналів можна при бажанні розглядати як корпорацію. Але сенс і труднощі корпоративного регулювання полягають у тому, що його суб'єктом виступає не колегія фахівців, а спільнота однодумців в організації, де працюють люди різних професій, статусів та інтересів.

Корпоративна етика - явище досить нове. Про неї можна говорити тільки з того моменту, коли в різних галузях господарської та соціальної діяльності стали домінувати великі компанії, побудовані за принципом скрупульозного поділу праці.

Термін "корпоративна етика" вживається в різних значеннях.

По-перше, в оціночному значенні - як високі моральні стандарти відповідають цим стандартам внутрішньоорганізаційних відносин і відносин організації зі стейкхолдерами (персоналом фірми, акціонерами, постачальниками, клієнтами, жителями населеного пункту, де розміщується компанія, і т.д.), групами осіб , на які впливає діяльність організації.

По-друге, як особливий спосіб морального регулювання ділових відносин у великих організаціях з анонімними відносинами, як один з інструментів підтримки або зміни організаційної культури.

По-третє, під корпоративною етикою розуміється дисципліна прикладної етики, яка вивчає моральні аспекти відносин в корпораціях, їх ціннісно-нормативний зміст і механізми втілення сформульованих суспільством моральних вимог і стандартів у реальні організаційні відносини. Корпоративна етика досліджує специфіку інституційного регулювання в організаціях, місце морального регулювання в системі різних способів нормативного регулювання. Вона вивчає розподіл і форми реалізації моральної відповідальності в корпорації; службові аномалії (фаворитизм, непотизм[19], мобінг, харассмент та ін.), їх причини, наслідки та шляхи подолання; види дискримінацій в організаціях, методи їх профілактики і боротьби з ними; структурні і особистісні причини адміністративних зловживань; а також займається етичним обґрунтуванням кордонів втручання в особисте життя працівника, розробкою методів захисту його прав в організації; досліджує проблеми ділового спілкування, пов'язані з відмінностями національних ділових культур, і методи їх вирішення та ін.

[19] Непоти́зм (італ. nepotismo від лат. nepos, род. відм. nepotis – «онук», «племінник») – надання родичам або знайомим посад незалежно від їхніх професійних здібностей Одна з частин політичної корупції, різновид фаворитизму. Інша назва – кумівство, тобто «потурання по службі своїм друзям або родичам на шкоду справі»

Окремим випадком служать сучасні транснаціональні компанії, чия діяльність протікає в масштабах всього світу. З цієї точки зору метою корпоративної етики можна вважати не збереження високих стандартів професії, а формування єдиного корпоративного духу в ситуації, коли деякі складові частини компанії розкидані в різних частинах світу. Очевидно, що в основу подібної об'єднуючої ідеології повинні бути покладені моральні цінності, посиланням на які корпорація могла б виправдати своє існування перед суспільством.

Висновок. У світі, де конкуренція на ринку праці стає все більш жорсткою, високий рівень професіоналізму є ключовим для успіху в будь-якій професії. Професійна та корпоративна етика є важливими складовими професіоналізму, оскільки вони сприяють формуванню високої моральної дисципліни, вмінню розв'язувати складні проблеми та приймати етичні рішення, а також створюють сприятливі умови для розвитку професіоналізму та успішної роботи в команді. Дотримання професійних та корпоративних етичних стандартів дозволяє працівникам бути впевненими в своїй роботі, підтримує довіру між колегами та забезпечує високу якість роботи.

Проте, варто зазначити, що професійна та корпоративна етика не є статичними концепціями. Їхні стандарти та принципи можуть змінюватись з часом в залежності від соціальних, культурних та технологічних тенденцій. Тому важливо здійснювати постійний моніторинг та оновлення професійних та корпоративних етичних стандартів для того, щоб вони відповідали сучасним реаліям.

Питання для самоконтролю:

1. У чому полягають найважливіші риси професійної етики?
2. Коли з’явилась корпоративна етика і чим вона відрізняється від професійної етики?
3. Які едоліки етичної теорії і практики?
4. Які особливості професійної етики?

Завдання:

1. Визначити професії, які визнаються еталоном моральності, та обґрунтувати їх моральність.

2. Підготувати приклади корпоративних кодексів організацій кібербезпеки.
3. Підготувати приклади професійних кодексів фахівців інформаційної безпеки.

1.3. Інформаційна етика як моральна регуляція сучасного суспільства

Сучасне суспільство має необмежений доступ до інформації завдяки швидкому розвитку технологій. Інформаційна етика – це набір принципів та правил поведінки, які регулюють використання, передачу та зберігання інформації в електронному вигляді. Інформаційна етика стала необхідною у зв'язку з тим, що у суспільстві збільшується кількість випадків порушення конфіденційності, крадіжки даних та вірусів, що шкодять інформаційній безпеці суспільтства та потребує його моральної регуляції.

Як здійснюється моральна регуляція сучасного суспільства?

У людини є моральні звички, коли моральних норм дотримуються автоматично, без зайвих роздумів. Це можливо в простих ситуаціях, якщо немає суперечностей та колізій, які потребують рефлексії[20] (допомогти слабкому, поступитися місцем людині похилого віку, захистити дитину тощо).

Але в деяких випадках звички виявляється недостатньо: є необхідною моральна рефлексія (роздуми, міркування, врахування «за» та «проти»). Наприклад, повідомити тяжкохворому про його хворобу, зробити вибір: допомога хворій матері чи захист Батьківщини тощо.

Інколи ми керуємося моральною інтуїцією (яка складається на основі попередніх роздумів та звичок). Мораль завжди існує як переживання, як живе почуття, яке спричиняє страждання або радість (що зумовлює інколи безпосередність реакцій). Ми можемо скільки завгодно умовляти себе,

[20] Рефле́ксія (від лат. reflexio – «повертаюся назад») – метод самоаналізу знань і вчинків, їх значень та меж. Наукова рефлексія орієнтована на критику й усвідомлення теоретичного знання; також досліджує способи та методи пізнання, які використовуються в тій чи іншій сфері досліджень. Філософська рефлексія сконцентрована на усвідомлені та пізнанні граничних основ буття, мислення та людської культури загалом. Літературна рефлексія – емоційне зрозуміння в художньому творі автором власних переживань, роздуми над динамікою душевного стану. Педагогічна рефлексія – наслідок взаємодії вчителя з учнем, який полягає у зворотньому зв’язку від учня після засвоєння масиву поданої вчителем інформації.
Рефлексія (програмування) – функціонал, який дозволяє отримати опис класу (назви, типи полів, аргументів, методів, а також модифікатори доступу), маючи лише його екземпляр.

пояснювати собі, переконувати, що вчинили добре, не зробили нічого поганого, але якийсь голос всередині буде не давати нам заспокоїтися.

Увага до морального почуття як визначального – етичний сенсуалізм[21], в основі моральної поведінки лежать моральнісні почуття: симпатія, взаємність, доброзичливість. Мораль здійснюється не лише в логіко-рефлексивній формі, а й в емоційній та підсвідомій формах. За способом свого буття мораль – це система норм, принципів, цінностей, якими керуються люди в своїй реальній поведінці.

Перш за все, мораль – це один із способів регуляції людських відносин, поведінки та свідомості.

Розвиток інформаційних технологій впливає на всі сторони життя сучасної людини. Інформаційні технології здійснюють величезний вплив на фундаментальні права людини стосовно захисту авторських прав, інтелектуальної свободи, відповідальності й безпеки.

Зростання інформаційної насиченості сучасного життя обернено пропорційно його духовно-моральному змісту. Це створює прецедент етичного аналізу ситуації, що склалася навколо сучасної фази технічної цивілізації і так званого "інформаційного суспільства", що є найбільш значущим результатом цього розвитку [12, 13].

Інформаційне суспільство – соціологічна концепція, що визначає головним фактором розвитку суспільства виробництво та використання науково-технічної та іншої інформації. Концепція інформаційного суспільства є різновидом теорії постіндустріального суспільства, засновниками якої були З. Бжезинський, Д. Белл, О. Тоффлер.

Поняття інформаційного суспільства найбільш повно аргументоване Д. Беллом[22] у теорії технологічного розвитку. На його думку у наступному столітті інформація, знання й кваліфікація суб'єкта стають головними факторами влади й управління. Вирішальне значення для економічного та соціального життя, для способів виробництва знання, а також для характеру трудової діяльності людини набуває становище нового соціального укладу, що базується на

[21] Сенсуалізм (від фр. sensualisme, лат. sensus – сприйняття, почуття, відчуття) – напрямок у теорії пізнання, згідно з яким відчуття й сприйняття – основна й головна форма достовірного пізнання. Суперечить раціоналізмові.
[22] Деніел Белл (англ. Daniel Bell, 10 травня 1919, Нью-Йорк, США – 25 січня 2011, Кембридж, Массачусетс, США) – соціолог і публіцист США, засновник теорії постіндустріального (інформаційного) суспільства.

телекомунікаціях. Революція в організації та обробці інформації та знань, в якій головну роль грає комп'ютер, розвертається водночас з розвитком індустріального суспільства. Три аспекти останнього особливо необхідні для розуміння телекомунікаційної революції:

- перехід від індустріального до сервісного суспільства;
- вирішальне значення кодифікованого теоретичного знання для здійснення технологічних інновацій;
- перетворення нової "інтелектуальної технології" у ключовий засіб системного аналізу та теорії приймання рішень [14].

З'являється нова інформаційна культура, які присутнє вміння працювати з інформацією, використовувати її, обробляти, зберігати й передавати. Нова культура спілкування відкриває нові форми особистих і професійних зв'язків за допомогою електронної пошти, www, телеконференцій, тобто без особистої присутності, але в режимі діалогу. В результаті такої діяльності формуються особливі етичні відносини, що сконцентровані у понятті «інформаціна етика».

Інформаці́йна е́тика (англ. Information ethics) - розділ прикладної етики, який має своїм предметом формування етичних стандартів та норм поведінки при створенні, поширенні та використанні інформації [15].

Певні етичні правила типу "не гарно читати чужі листи" формувалися в давні часи. Бібліотекарі, архівісти та інші працівники інформаційної сфери стикалися з етичними конфліктами та етичними дилемами задовго до того, як цифрові медіа та Інтернет почали змінювати інформаційну сферу. Афоризм Френсіса Бекона[23] «Знання це сила» вказує на той факт, що обмежений доступ до інформації та обмежена освіта були і є передумовами панування правлячих еліт у недемократичних суспільствах.

Особливого значення дослідження в галузі інформаційної етики набувають в сучасний період. Інформаційна етика пов'язана з комп'ютерною етикою і філософією інформації.

Філосо́фія інформа́ції - область дослідження, яка вивчає концептуальні питання, що виникають на перетині філософії, кібернетики, інформаційних технологій. Вона включає в себе:

- критичні дослідження концептуального характеру та основні принципи інформації, в тому числі її динаміки, використання і науки

[23] Фре́нсіс Бе́кон (англ. Francis Bacon, 22 січня 1561, Лондон – 9 квітня 1626) – англійський політик, державний діяч, вчений, філософ і есеїст. Лорд-хранитель Малої печатки і Лорд-канцлер Англії в 1617–1621 роках. Один із творців емпіризму – філософського напряму, який твердить, що головне – власний досвід.

- розробка і застосування теоретичної інформатики та обчислювальних методів у філософських проблемах.

Деякі посилання філософії інформації можна знайти в технічних роботах Норберта Вінера, Алана Тюринга, Вільяма Росса-Ешбі, Клода Шеннона, Воррена Вівера і багатьох інших вчених, що працюють над інформаційно-обчислювальною теорією ще з початку 1950-х років.

Інформаційна етика розглядає проблеми власності, доступу, приватності, безпеки й доступності інформації.

Одним з головних принципів інформаційної етики є повага до приватності та конфіденційності інформації. Цей принцип вимагає, щоб приватна інформація була збережена в таємниці та не була використана без згоди її власника. Наприклад, лікарі та адвокати повинні дотримуватися таємниці, щоб забезпечити захист особистої інформації своїх пацієнтів та клієнтів.

Інший важливий принцип інформаційної етики – це заборона крадіжки та плагіату інформації. Цей принцип вимагає, щоб будь-яка інформація, яка використовується, була правильно цитована та вказані автори та джерела. Це дуже важливо для забезпечення належної кредитної гідності, а також для захисту авторських прав.

Крім того, інформаційна етика включає в себе відповідальне використання та передачу інформації. При цьому повинні дотримуватися різні принципи, такі як відповідність, точність, дослідження джерел та забезпечення безпеки. Наприклад, журналісти повинні збирати та передавати інформацію відповідно до принципів об'єктивності та нейтральності.

Інформаційна етика також включає в себе заборону на розповсюдження неправдивої, образливої та дискримінаційної інформації. Цей принцип вимагає поваги до інших та захисту їх прав. Наприклад, викладачі та студенти повинні уникати розповсюдження образливих та дискримінаційних коментарів в соціальних мережах.

Інформаційна етика також включає в себе забезпечення безпеки та захисту інформації. Цей принцип вимагає використання надійних методів збереження та передачі інформації. Наприклад, користувачі мережі Інтернет повинні зберігати свої паролі та іншу конфіденційну інформацію в таємниці та не ділитися ними з іншими особами.

На фоні глобалізації сучасного світу особливе значення мають питання інформаційної етики на фоні міжнаціональних, міжкультурних та

міжконфесійних відносин. Одним із основних завдань інформаційної етики в сучасних умовах простого і широкого доступу кожної людини до інформаційного поля є розробка правил ведення дискусій в інтернеті, які, на жаль, часто ведуться з використанням ненормативної лексики.

Інформаційна етика тісно пов'язана з інформаційною безпекою, яка у свою чергу є складовою частиною національної безпеки. Неетичні дії у інформаційній сфері можуть складати загрозу інформаційній безпеці людини, суспільства, держави.

Важливою складовою сучасної інформаційної етики є журналістська етика. Журналі́стська е́тика - набір правил і норм поведінки, яких мають дотримуватися всі, хто збирає, опрацьовує та поширює масову інформацію [16, 17]. Прийнятий на З'їзді журналістів 12 грудня 2013 року Кодекс етики українського журналіста визначає основні морально-етичні орієнтири, яких журналіст має дотримуватися при виконанні своїх професійних обов'язків, і являє собою 19 моральних принципів фахової діяльності [16]:

1. Свобода слова та висловлювань є невід'ємною складовою діяльності журналіста.

2. Служіння інтересам влади, а не суспільства є порушенням етики журналіста.

3. Журналіст має з повагою ставитися до приватного життя людини.

4. Висвітлення судових процесів має бути неупередженим щодо звинувачених. Журналіст не може називати людину злочинцем до відповідного рішення суду.

5. Журналіст не розкриває своїх джерел інформації, окрім випадків, передбачених законодавством України.

6. Повага до права громадськості на повну та об'єктивну інформацію про факти і події є найпершим обов'язком журналіста.

7. Інформаційні та аналітичні матеріали мають бути чітко відокремлені від реклами відповідною рубрикацією.

8. Редакційна обробка матеріалів, включаючи знімки, текстівки, заголовки, відповідність відеоряду й текстового супроводу тощо не повинні фальсифікувати зміст.

9. Факти, судження і припущення мають бути чітко відокремлені одні від одного.

10. Думки опонентів, зокрема тих, хто став об’єктом журналістської критики, мають бути представлені збалансовано. Так само мають бути подані оцінки незалежних експертів.

11. Не допускається таке вибіркове цитування соціологічних досліджень, яке призводить до викривлення змісту. Журналістські опитування громадян не повинні фабрикуватися з метою отримання наперед визначеного результату.

12. Журналіст зобов’язаний зробити все можливе для виправлення будь-якої поширеної інформації, якщо виявилося, що вона не відповідає дійсності.

13. Журналіст не повинен використовувати незаконні методи отримання інформації. Журналіст під час збирання інформації діє і правовому полі України і може вдатися до будь-яких законних, зокрема судових, процедур проти осіб, які перешкоджають йому в зборі інформації.

14. Плагіат несумісний зі званням журналіста.

15. Ніхто не можу бути дискримінований через свою стать, мову, расу, релігію, національне, регіональне чи соціальне походження або політичні уподобання. Указувати на відповідні ознаки особи (групи людей) слід лише у випадках, коли ця інформація є неодмінною складовою матеріалу.

16. Журналіста не можна у службовому порядку зобов’язати писати чи виконувати будь-що, коли це суперечить його власним переконанням чи принципам.

17. Незаконне отримання журналістом матеріальної винагороди чи будь-яких пільг за виконаний чи невиконаний журналістський матеріал є несумісним за званням журналіста.

18. Журналіст має бути особливо обережним при висвітленні питань, пов’язаних із дітьми. Журналіст і редактор повинні мати обґрунтовані підстави для висвітлення приватного життя неповнолітньої особи (осіб) та дозвіл на це від її батьків чи опікунів. Неприпустимим є розкриття імен неповнолітніх (або вказування ознак, за якими їх можна розпізнати), які мали стосунок до протизаконних дій, стали учасниками подій, пов’язаних із насильством.

19. Журналіст має бути патріотом України: не шкодити своєю діяльністю інтересам держави, боротися з внутрішніми та міжнародними проявами неповаги до наших національних і християнських цінностей (мови, культури, літератури, історії, звичаїв і традицій), відстоювати українську незалежність і територіальну цілісність.

Ці 19 принципів написані на основі прав і свобод людини, викладених у Загальній декларації прав людини, Всесвітній Хартії свободи преси ООН, Декларації принципів поведінки журналіста Міжнародної Федерації журналістів, Конституції України та чинного законодавства.

У будь-якому випадку етичні конфлікти та дилеми не є новим явищем інформаційного суспільства. Але інформаційні технології, засновані на комп'ютерах, цифрових засобах масової інформації та Інтернеті, посилили потенціал серйозного порушення фундаментальних цінностей, пов'язаних із інформаційною етикою. Квазімонопольні Інтернет-компанії, такі як Google, Bing або Yahoo, мають можливість маніпулювати результатами пошуку своїх користувачів, не ризикуючи бути виявленими у кожному конкретному випадку. Соціальні мережі, такі як Facebook, WhatsApp тощо здатні збирати та продавати персональні дані.

Перехід України до інформаційного суспільства зумовлює зростання ролі людського потенціалу як головного ресурсу, мети і критерію соціально-економічного розвитку. Даний процес вимагає певної систематизації теоретичного надбання сучасних українських і зарубіжних учених та виявлення основних тенденцій розвитку наукових парадигм теорії людського розвитку. Людський розвиток розглядається і як процес розширення людського вибору, і як досягнутий рівень добробуту людини. Однак ще досі головні засади Концепції розвитку людського потенціалу не реалізовані в Україні. Розвиток інформаційного суспільства в Україні є сьогодні не так інструментально-технологічною, скільки інформаційно-психологічною проблемою, для вирішення якої необхідно змінити суспільну свідомість і, в першу чергу, чиновників. Формуванню інформаційного суспільства сьогодні немає альтернативи. Це магістральний напрям розвитку цивілізації в 21-му столітті, за яким вже йдуть всі розвинені і багато країн світу, що розвиваються. Адже саме завдяки пріоритетному інформаційному розвитку в останні роки домоглися досить вражаючих економічних успіхів такі країни, як Фінляндія, Норвегія, Швеція, які за величиною валового внутрішнього продукту на душу населення увійшли до першої десятки країн світу.

При безсумнівних успіхах сучасної техніки, що досягла найбільш вражаючих результатів у галузі інформаційних технологій, у середовищі філософського співтовариства росте непідробна тривога у зв'язку з моральними небезпеками людському існуванню, які є наслідком науково-технічного

розвитку. Свою заклопотаність сьогодні виражають не тільки професійні філософи-етики, але й представники гуманітарної та технічної інтелігенції, політичні і громадські діячі, взагалі, всі мислячі, небайдужі люди [14].

Однак наслідки технологічного прориву виявилися настільки значними, що призвели до зміни сформованої системи відносин між людьми, породили особливу електронну форму культури, викликали нові екзистенційні[24] та етичні проблеми, з якими зіткнулась сучасна людина.

Непорушність інформаційної свободи, яка лежить сьогодні в основі культури віртуальної комунікації, дозволяє використовувати інформаційний простір в різних цілях, не зважаючи не моральні норми суспільства. Такий стан справ потребує величезних зусиль у проведенні досліджень науковців з етики як практичного так і теоретичного характеру [18].

Таким чином, загальносвітовою тенденцією є трансформація індустріального суспільства у постіндустріальне, що відбувається в умовах посилення глобалізаційних процесів, розширення сфери послуг і нематеріального виробництва у результаті науково-технічного прогресу, у тому числі масштабного, глибинного та динамічного проникнення інформаційно-комунікаційних технологій в усі сфери життєдіяльності особи, суспільства, суб'єктів господарювання та держави, в тому числі і у моральну сферу.

Не зважаючи на проблеми, що перешкоджають розвитку інформаційного суспільства в Україні, з метою стратегічного розвитку е-культури необхідно здійснювати заходи щодо підтримки діяльності державних та інших організацій із збереження в суспільстві культурних і моральних цінностей, традицій патріотизму і гуманізму з використанням інформаційно-комунікаційних технологій [19].

Висновок. Інформаційна етика є дуже важливим фактором для забезпечення ефективного використання та збереження інформації в електронному вигляді. Поважання прав на приватність та авторських прав, відповідальне використання та передача інформації, заборона на розповсюдження неправдивої та образливої інформації, а також забезпечення безпеки та захисту інформації - це лише деякі принципи інформаційної етики, які допомагають підтримувати моральні стандарти в електронному світі.

[24] Екзистенціалі́зм або філософія існування (фр. existentialisme від лат. exsistentia – існування) – напрям у філософії XX століття, що позиціонує і досліджує людину як унікальну духовну істоту, що здатна до вибору власної долі.

З іншого боку, порушення інформаційної етики може мати серйозні наслідки для індивідуумів, організацій та суспільства в цілому. Неправдива або образлива інформація може призвести до розголосу та негативних наслідків для людей, або викликати ризик відкликання товарів або послуг. Порушення конфіденційності або безпеки інформації може призвести до витоку конфіденційної інформації та збитків, або поставити людей під загрозу віддаленого доступу до їхніх особистих даних.

Отже, інформаційна етика не лише допомагає забезпечувати моральні стандарти в електронному світі, але і має важливе значення для безпеки та захисту прав людей та організацій. Важливо, щоб кожен, хто має справу з інформацією, дотримувався принципів інформаційної етики та виконував свої обов'язки відповідально, щоб забезпечити надійне та ефективне використання та збереження інформації.

 *Питання для самоконтролю*:

1. Як розвиток інформаційних технологій вплинув на етичні відносини у суспільстві?
2. Де закріплені етичні норми професійної діяльності?
3. В чому суть дилеми журналістської етики?
4. Як за допомогою інформаційних технологій можна регулювати суспільні відносини у державі?
5. Які етичні механізми для регулювання суспільних відносин уже існують?

 *Завдання:*

1. За допомогою Інтернету знайти етичні кодекси професії лікаря та педагога.

1.4. Поняття, принципи комп'ютерної етики

В найзагальнішому сенсі Комп'ютерна етика займається дослідженням поведінки людей, що використають комп'ютер, на основі чого виробляються відповідні моральні приписи й своєрідні норми етики. Саме вживання терміну «комп'ютерна етика» досить умовне, ця дисципліна дуже молода, вона з'явилася на межі 70-х – 80-х рр. XX сторіччя, і поряд з нею вживаються такі терміни, як «інформаційна етика», «кіберетика».

Комп'ютерна етика являє собою область міждисциплінарного дослідження й включає розгляд технічних, моральних, юридичних, соціальних, політичних і філософських питань. Проблеми, аналізовані в ній, умовно можна розділити на кілька класів:

- проблеми, пов'язані з розробкою моральних кодексів для комп'ютерних професіоналів і простих користувачів, чия робота пов'язана з використанням комп'ютерної техніки;
- проблеми захисту прав власності, авторських прав, права на особисте життя й волю слова стосовно області інформаційних технологій;
- група проблем, пов'язаних з появою комп'ютерних злочинів, визначенням статусу, тобто переважно правові проблеми.

Джеймс Мур, один із першодослідників комп’ютерної етики у статті “Що таке мережева етика?” писав: “XX століття – це епоха комп’ютерної революції, в якій можна розрізняти дві стадії. Перша стадія пов’язана зі створенням і вдосконаленням власне ЕОМ, друга полягає в тому, що інформаційно комп’ютерні технології швидко стають інтегрованою частиною ледь не для всіх суспільних інститутів”. **Комп'ютерна етика за Джеймсом Муром** – це складне динамічне поле досліджень, що передбачає аналіз відносин між фактами, концепціями, політикою і цінностями в контексті інтенсивного розвитку інформаційно-комп'ютерних технологій. Він визначає комп'ютерну етику як "аналіз природи соціального впливу комп'ютерних технологій на суспільство, формулювання на цій основі моральних норм і проведення активної політики їх впровадження у свідомість розробників і користувачів комп'ютерних технологій" [20]. Джеймс Мур у своїй роботі відзначає, що перетворення інформаційно-комп'ютерних

технологій в інтегровану частину практично всіх суспільних інститутів викликало широкий спектр глобальних проблем, які і стали предметом дослідження комп'ютерної етики. На його думку, ці проблеми виникають через відсутність ясності у питаннях стосовно етичних обмежень при вживанні комп'ютерних технологій та невизначеність вчинків при використанні нових можливостей у виборі дій, наданих комп'ютерами суспільству. Філософ наголошує, що комп'ютерна етика покликана сформулювати правила цих нових дій і відповісти на питання етичного застосування комп'ютерних технологій як соціального, так й особистісного характеру.

Оскільки операції комп'ютера, як правило, «невидимі», Джеймс Мур виділив три класи комп'ютерних «невидимих» чинників, що мають етичне значення.

Першим типом «невидимого чинника» він назвав «невидимий обман», тобто навмисне використання невидимих операцій комп'ютера з метою здійснити неетичну або злочинну дію. У зв'язку з цим він наводить такий гіпотетичний приклад. Під час банківських операцій при підрахунку відсотків із внесків після округлення сум постійно залишаються долі проценту. Програміст міг би скласти і ввести у комп'ютер відповідну програму із завданням переводити ці залишкові долі з усіх банківських операцій на свій рахунок, здійснивши тим самим викрадення «надмірного відсотка».

Другим типом «невидимого чинника» у комп'ютерній технології є, на думку Джеймса Мура, присутність «невидимих цінностей програми», тобто цінностей, що ненавмисно вводяться до програми і до певного часу не відомі ні її користувачам, ні розробникам. Так при створенні програми для попереднього продажу авіаквитків у США у 80-і рр. програмісти використовували алфавітний принцип. Ця «невидима цінність програми» залишалася непоміченою, доки не з'ясувалося, що при продажу авіаквитків компанія «Америкен ейрлайнз» одержувала перевагу перед компанією «Бреніфф ейрлайнз», що призвело до банкрутства останньої і скінчилося судовим розглядом.

Третій тип «невидимого чинника» комп'ютерної технології - «невидимий комплекс обчислень». Справа в тому, що комп'ютер здатний виконувати такі складні розрахунки, які просто не охоплюються людською свідомістю, незбагненні для людського розуміння і непідвладні контролю (навіть якщо сама програма цілком доступна нашому інтелекту). Дж. Мур вказує, що звідси виникає питання, наскільки можна довіряти «невидимому розрахунку».

Американський етик Дебора Джонсон випустила підручник "Комп'ютерна етика" (1985 р.), який в 1994 р. вийшов другим виданням [21]. Її вважають засновником комп'ютерної етики як навчальної дисципліни, яку необхідно розпочинати викладати, на її думку, ще з дитячого садку і потім продовжувати - в навчальних закладах різних рівнів. Комп'ютерна етика за Деборою Джонсон – розглядається як навчальна дисципліна та охоплює етичні проблеми інформаційно-комп'ютерних технологій, що мають спиратися на традиційні моральні принципи і теорії. Комп'ютерна етика розуміється як поле досліджень, розташоване на межі між новими технологіями і нормативною етикою; фахівці її розглядають одночасно і як дослідницький напрям.

Поряд с поняттям «комп'ютерна етика» став поширюватися вислів «етика Інтернет», «мережевий етикет» або «нетикет» (net – у перекладі з англ. мови це – мережа); такі поняття можна зустріти й у електронних практичних посібниках для користувачів Інтернету, і в правилах, встановлених на веб-сайтах, наприклад у чатах, на форумах мережі. Один з американських сайтів так і називався – «webethics», тобто «етика Інтернет» (до речі, американці називають весь інтернет узагальненим словом «Веб») [20, 22]. Принципи комп'ютерної етики наступні:

- privacy (таємниця приватного життя) – право людини на автономію й свободу в приватному житті, право на захист від вторгнення в неї органів влади й інших людей;
- accuracy (точність) – дотримання норм, пов'язаних з точним виконанням інструкцій для експлуатації систем і обробці інформації, чесним і соціально-відповідальним відношенням до своїх обов'язків;
- property (приватна власність) – недоторканність приватної власності – основа майнового порядку в економіці, принцип означає дотримання права власності на інформацію й норм авторського права;
- accessibility (доступність) – право громадян на інформацію, її доступність у будь-який час і в будь-якому місці.

Заповіді комп'ютерної етики. (ISC)²[25] - професійна асоціація, яка прагне створити безпечний і безпечний кіберсвіт, додатково визначила власний кодекс етики. Кодекс заснований на канонах під загальною преамбулою.

[25] (ISC)² чи The International Information System Security Certification Consortium (укр. Міжнародний консорціум з сертифікації в галузі безпеки інформаційних систем) – міжнародна некомерційна організація з тестування і сертифікації фахівців в галузі інформаційної безпеки. Вона була названа «найбільшою в світі організацією з безпеки IT»

Преамбула кодексу етики. Безпека та добробут суспільства та загальне благо - обов’язок перед нашими принципами та один перед одним вимагають, щоб ми дотримувались найвищих етичних стандартів поведінки. Тому суворе дотримання цього Кодексу є умовою сертифікації діяльності.

Етичний кодекс канонів включає:

- перший канон: захищайте суспільство, загальне благо, необхідну громадську довіру та впевненість, а також інфраструктуру;
- другий канон: дійте чесно, чесно, справедливо, відповідально та законно;
- третій канон: розвивайте та захищайте професію.

Найяскравіше своє втілення комп'ютерна етика одержала в області розробки моральних кодексів. Досить показове відношення до розглянутої проблеми у США, де перший кодекс комп'ютерної етики був розроблений в 1979 році. Прийняття кодексу було продиктовано розумінням того, що інженери, вчені й технологи результатами своєї діяльності визначають якість і умови життя всіх людей в інформаційному суспільстві. Тому в преамбулі кодексу підкреслюється життєво важлива необхідність дотримання всіх норм етики при розробці й експлуатації засобів інформаційних технологій. Згодом були розроблені й прийняті кодекси в багатьох інших організаціях США, зв'язаних зі сферою інформаційних технологій, таких як:

- «Асоціація розробників комп'ютерних технологій» (ACM);
- «Асоціація менеджерів інформаційних технологій» (DPMA);
- «Асоціація користувачів інформаційних технологій у США» (ITAA);
- «Асоціація сертифікованих комп'ютерних професіоналів» (ICCP).

На основі етичних стандартів, використовуваних у кодексах, «Міжнародна федерація з інформаційних технологій» (IFI) рекомендувала прийняти кодекси комп'ютерної етики національним організаціям інших країн з урахуванням місцевих культурних і етичних традицій. Зміст окремих кодексів може відрізнятися один від одного, але в їхній основі повинен лежати деякий інваріантний набір моральних установок, які умовно можуть бути зведені до наступного:

- не використовувати комп'ютер з метою шкоди іншим людям;
- не створювати перешкод і не втручатися в роботу інших користувачів комп'ютерних мереж;

- не користуватися файлами, не призначеними для вільного використання;
- не використовувати комп'ютер для злодійства;
- не використовувати комп'ютер для поширення помилкової інформації;
- не використовувати крадене програмне забезпечення;
- не привласнювати чужу інтелектуальну власність;
- не використовувати комп'ютерне устаткування або мережеві ресурси без дозволу або відповідної компенсації;
- думати про можливі суспільні наслідки програм, які ви пишете, або систем які ви розробляєте;
- використовувати комп'ютер із самообмеженнями, які показують вашу люб'язність і повагу до інших людей.

Не зважаючи на те, що дотримання моральних норм підтримується тільки силою суспільного впливу, їх наявність необхідна і тому, що історично на основі норм моралі виробляються нові й удосконалюються існуючі юридичні норми, які забезпечуються державним впливом.

В українському суспільстві вже починають звертатися до проблем та питань, що виникають паралельно з швидким проникненням Інтернет-технологій в суспільне життя і, зокрема, в освітню сферу, де новітні технології стають інструментом інтерактивного навчання, особливо в напрямі розвитку дистанційної освіти [23]. І в цьому напрямі одним із сучасних завдань має стати впровадження в освітні заклади навчальної дисципліни «Комп'ютерна етика» як для користувачів, так і для фахівців розробників комп'ютерних систем і мереж в будь-якій сфері людської діяльності. Для фахівців спеціальності «Кібербезпека» розроблений даний посібник, який містить базові теоретичні знання, необхідні для забезпечення цілісного уявлення щодо розуміння проблем професійної та корпоративної етики в управлінні кібербезпекою.

Морально-етичні принципи інформаційної культури будь-якого учасника інформаційно-мережевого середовища є вкрай важливими й необхідними для комфортного співіснування «людина-комп’ютер-інтернет», для створення загальних позитивних результатів користування інформаційними ресурсами з будь-якої сфери сучасного соціального суспільства.

 *Питання для самоконтролю*:

1. Назвіть принципи комп’ютерної етики.

2. Які проблеми аналізуються в комп’ютерній етиці?
3. В чому суть комп'ютерної етики за Джеймсом Муром?
4. В чому суть комп'ютерної етики за Деборою Джонсон?
5. Де і коли був розроблений перший кодекс комп’ютерної етики?

Завдання:

1. За допомогою Інтернету знайти зразки комп’ютерних кодексів.
2. Підготувати етичні положення для формування компютерного кодексу в організації кібербезпеки , де циркулює інформація з обмеженим доступом.

1.5. Етика науково-педагогічної діяльності

Демократичні зміни в сучасному суспільстві України зумовили відхід від авторитарних стереотипів у сфері освіти, що вимагає від викладача пошуків і розробки засад, форм, методів і прийомів в організації та здійсненні такого педагогічного процесу на всіх рівнях.

Науково-педагогічна етика - це сукупність етичних принципів та стандартів поведінки в галузі науки та освіти, які регулюють взаємовідносини між викладачами, науковцями, студентами, колегами та іншими учасниками цих сфер. Ці принципи включають у себе дотримання наукової доброчесності, відповідальності, справедливості та поваги до прав людини.

Педагогічна культура викладача потребує опанування демократичним стилем спілкування зі студентами. Здатність до міжособистісного спілкування, ведення діалогу, переговорів, тактовність, стиль поведінки, формування інтелектуального та культурного потенціалу держави, етикет є одним із стратегічних завдань, як зазначено у законі України "Про освіту" [23], "Національній доктрині розвитку освіти України у XXI столітті" [24].

Значення професійної етики в регулюванні різних видів трудової діяльності пов'язано з прагненням постійно вдосконалювати норми поведінки згідно з суспільними відносинами, що постійно змінюються. Тому важливою складовою підготовки сучасного фахівця стає знання нормативної та професійної етики, що регламентує поведінку людей у навчальних закладах на

службі, у громадських місцях, на різного роду офіційних заходах - прийомах, церемоніях, переговорах.

Так, римський оратор Марк-Фабій Квінтіліан[26] (прибл. 35 - прибл. 96 рр.)

обґрунтував важливість вибору такого вчителя, у якого моральність на першому місці, адже аморальний педагог виховує подібну до себе аморальну дитину. Досвідчений учитель передусім вивчає розумові та природні нахили, здібності дитини, щоб знати, як поводитися з нею, уникнувши тілесних покарань. Насилля, знущання над дитиною засвідчують недостатній духовний зв'язок педагога зі своїм учнем, продукують моральне приниження учня і вчителя, формують рабську психологію.

Марк-Фабій Квінтіліан розробив кодекс педагогічної етики. Його дотримання має виховувати повагу і шану до вчителя. До основних положень його кодексу належать такі:

1. Нехай учитель викличе в собі батьківські почуття до своїх учнів і постійно уявляє себе на місці тих людей, які довіряють йому своїх дітей.

2. Нехай він сам не має вад і не переносить їх на інших.

3. Нехай суворість його не буде гнітючою, а ласкавість – розслабливою, щоб звідси не виникли ненависть або презирство.

4. Нехай будуть тривалими бесіди про моральне й добре, адже чим частішими будуть умовляння, тим меншою – потреба в покараннях.

5. Нехай учитель не буде роздратованим і водночас не потурає тим, хто потребує виправлення.

6. Нехай він буде доступним у викладанні, терплячим у роботі, більш старанним, ніж вимогливим.

7. Нехай із бажанням відповідає тим, хто запитує, і нехай запитує мовчазних.

8. На похвалу нехай не буде надто скупим, оскільки це знищує бажання до праці, але й не буде надто щедрим, що породжує безпечність.

9. Наставляючи учня, він не повинен бути надто суворим, тим більше сварливим. Адже в багатьох з'являється відраза до педагога через те, що докори деяких учителів перетворюються на ненависть.

[26] Марк Фабій Квінтиліан (лат. Marcus Fabius Quintilianus) – найвідоміший із римських педагогів, ритор (вчитель красномовства), автор «Повчання оратору» (лат. Institutio oratoria) – найповнішого підручника ораторського мистецтва, який дійшов до нас з античності.

10. Нехай він кожен день скаже учням що-небудь таке, що в них назавжди залишиться в пам’яті.

Педагогічна етика - розділ професійної етики, який вивчає сутність і зміст, особливості педагогічної моралі, обґрунтовує п категорії, норми, принципи, функції у процесі педагогічної діяльності.

Предметом педагогічної етики є особливості вияву моралі у свідомості, поведінці, професійній діяльності педагога і його відносинах з учнями, батьками та колегами. До змістових структурних компонентів педагогічної етики належать моральна свідомість, моральна діяльність і моральні відносини.

Моральна свідомість - форма суспільної свідомості, яка відображена і закріплена у вигляді моральних норм і правил поведінки людей у суспільному й особистому житті. Структуру моральної свідомості утворюють основні елементи: моральні знання; моральні почуття.

Моральні знання є особливою формою духовного засвоєння результатів пізнання, процесу відображення дійсності з погляду моральності (добра, справедливості, гідності), яка характеризується усвідомленням їх істинності.

Моральні почуття – форма суб'єктивного, безпосереднього переживаного морального ставлення особистості до явищ навколишньої дійсності, інших людей і їхніх вчинків, самої себе і власних дій.

Педагогічна мораль – система етичних вимог, що постає перед викладачем в його ставленні до самого себе, до своєї професії, до суспільства, до дітей і решти учасників навчально-виховного процесу.

Моральна діяльність охоплює не лише просвітництво, самовиховання і досвід, а й мету, потреби, мотиви, засоби та результат діяльності. Моральні відносини представлені на рівні відносин з учнем (учнівським колективом), колегами і керівництвом школи, батьками і суспільством.

Педагогічний такт – це педагогічно грамотне спілкування в складних педагогічних ситуаціях, уміння знайти педагогічно доцільний і ефективний спосіб впливу, відчуття міри, швидкість реакції, здатність швидко оцінювати ситуацію і знаходити оптимальне рішення.

Педагогічний такт також виявляється в умінні керувати своїми почуттями, не втрачати самовладання, емоційну врівноваженість у поєднанні з високою принциповістю та вимогливістю, з чуйним людяним ставленням до студента. Він вимагає критичності і самокритичності в оцінці своєї праці, нетерпимості до

шаблону, формалізму, застою думки і справи, до бюрократизму і пихи, поваги. Педагогічний такт реалізується через мову і стиль поведінки.

Основні показники педагогічного такту науково-педагогічного працівника включають [25]:

- людяність без зарозумілості;
- вимогливість без брутальності та причепливості;
- педагогічний вплив без наказів, навіювань, попереджень, без приниження особистої гідності студента;
- вміння висловлювати розпорядження, вказівки та прохання без зухвалості, без зарозумілості;
- уміння слухати співрозмовника, не виявляючи байдужості та вищості;
- урівноваженість, самовладання і діловий тон спілкування, без дратівливості та сухості;
- простота в спілкуванні без фамільярності та панібратства, без показухи;
- принциповість і наполегливість без упертості;
- уважність, чутливість і емпатичність без їх підкреслення;
- гумор без посміху;
- скромність без удаваності.

Удосконаленню педагогічного такту науково-педагогічного працівника сприяє так званий соціальний інтелект, який трактують як особливу індивідуальну рису, що дає змогу розуміти студента, усвідомлювати мотивацію його поведінки, розпізнавати найсуттєвіші риси індивідуальності. Ця якість виявляється як:

- просоціальна спрямованість, готовність до співпраці, особиста зацікавленість у добробуті інших;
- соціальна ефективність як очікування успіху в розв'язанні міжособистісних проблем;
- емпатичний інтерес та особисте співчуття, які забезпечують декодування невербальних ознак емоційних переживань;
- адекватне визначення ціннісних аспектів ставлення до себе й до інших.

Отже, педагогічний такт виховують, його набувають разом з педагогічною культурою і він виявляється в педагогічній діяльності. Він є показником зрілості науково-педагогічного працівника як майстра своєї справи. Це великий засіб, за допомогою якого студентів можна перетворити на своїх спільників чи, навпаки, суперників.

Педагогічна етика [25] розглядає сутність основних категорій педагогічної моралі й моральних цінностей. Моральними цінностями вважають систему уявлень про добро і зло, справедливість і честь, які виступають своєрідною оцінкою характеру життєвих явищ, етичних достоїнств і вчинків людей тощо. До педагогічної діяльності застосовуються всі основні моральні поняття, проте окремі поняття відображають такі риси педагогічних переконань, діяльності й відносин, які виділяють педагогічну етику у відносно самостійний розділ етики. Серед цих категорій – професійний педагогічний обов'язок, педагогічна справедливість, педагогічна честь і педагогічний авторитет.

Справедливість взагалі характеризує відповідність між достоїнствами людей і їх суспільним визнанням, правами і обов'язками. Педагогічна справедливість має специфічні риси, будучи своєрідною мірою об'єктивності вчителя, рівня його етичної вихованості (доброти, принциповості, людяності), що виявляється в його оцінках вчинків учнів, їх ставленні до навчання, проявах суспільно корисної діяльності тощо. Справедливість – це моральна якість вчителя і оцінка міри його впливу на учнів, що відповідає реальним заслугам перед колективом. Специфіка педагогічної справедливості полягає у такому: оцінка дії (відповідна реакція на неї) знаходиться у педагога і учня на різних рівнях етичної зрілості; визначення об'єктивності залежить здебільшого від педагога; загальній моральній оцінці піддається взаємодія сторін з нерівним самозахистом; педагогічно необхідне, запрограмоване педагогом, може не усвідомлюватися учнями.

Професійний педагогічний обов'язок – одна з найважливіших категорій педагогічної етики. У цьому понятті концентруються уявлення про сукупність вимог і моральних розпоряджень, що ставляться суспільством до особи викладача, а також виконання викладачем професійних обов'язків. Серед даних вимог такі: здійснювати певні трудові функції, переважно інтелектуальні, правильно будувати взаємостосунки з учнями, їх батьками, колегами по роботі, глибоко усвідомлювати своє ставлення до вибраної професії, учнівського і педагогічного колективу й суспільства в цілому. Основою професійного педагогічного обов'язку є об'єктивні та актуальні потреби суспільства в навчанні й вихованні підростаючих поколінь. У професійному обов'язку педагога запрограмована необхідність творчого ставлення до своєї праці, особлива вимогливість до себе, прагнення до поповнення професійних знань і підвищення педагогічної майстерності, необхідність поважного і вимогливого ставлення до

учнів і їхніх батьків, уміння вирішувати складні психологічні колізії та конфлікти.

Професійна честь в педагогіці – це поняття, що виражає не тільки усвідомлення вчителем своєї значущості, але і суспільне визнання, суспільну пошану його моральних заслуг і якостей. Високо розвинуте усвідомлення індивідуальної честі й особистої гідності в професії педагога чітко визначається. Якщо викладачем у своїй поведінці та міжособистісних відносинах порушуються вимоги, що ставляться суспільством до ідеалу педагога, то відповідно ним демонструється зневага до професійної честі й гідності. Честь викладача – суспільна оцінка його реальних професійних достоїнств, що виявляються в процесі виконання ним професійного обов'язку.

Педагогічний авторитет викладача – це його моральний статус у колективі учнів і колег, своєрідна форма дисципліни, за допомогою якої авторитетний і шановний педагог, регулює поведінку учнів, впливає на їх переконання. Педагогічний авторитет залежить від попередньої морально-етичної і психолого-педагогічної підготовки викладача. Рівень його визначається глибиною знань, ерудицією, майстерністю, ставленням до роботи тощо.

Культура вербального і невербального спілкування викладача вищої школи. Вербальне і невербальне спілкування. Вербальне - спілкування за допомогою мови і мовлення. Одна з найважливіших проблем цього типу спілкування - розуміння. Розуміння сенсу і значень слів залежить від розуміння понять, від обізнаності досвіду, спрямованості, ціннісних орієнтацій партнерів. За допомогою слів люди програмують свою поведінку і поведінку інших. У безпосередньому усному вербальному спілкуванні важливу роль відіграє інтонація, за допомогою якої партнери виділяють ключові слова, підкреслюють сенс фрази. Люди довіряють більш інтонації, ніж об'єктивному мовному виразу. Інтонація також використовується для вираження емоцій. Невербальне спілкування полягає в передачі і одержуванні інформації за допомогою міміки, пантоміміки, різного роду сигналів і символів. Велике значення в невербальному спілкуванні має мова погляду (тривалість погляду, тип погляду, розмір зрачка, якість, зміст погляду). Погляд передає не лише емоції, а також і змістовну інформацію. У невербальній комунікації люди послуговуються жестами. Жестикулюють намірено і спонтанно.

Невід'ємною складовою характеристики сучасного викладача є *рівень* його *педагогічної культури*. Педагогічна культура є частиною загальнолюдської

культури, в якій з найбільшою повнотою відображені духовні і матеріальні цінності освіти та виховання, а також способи творчої педагогічної діяльності, необхідні для обслуговування історичного процесу зміни поколінь, соціалізації особистості і здійснення освітньо-виховного процесу. Педагогічна культура інтегрує історико-культурний педагогічний досвід і регулює сферу педагогічної взаємодії.

У культурно-історичному аспекті вона містить світовий педагогічний досвід як зміну світових культурних епох і відповідних їм педагогічних цивілізацій, як історію педагогічної думки науки і освіти.

У соціально-педагогічному аспекті педагогічна культура постає як явище соціальне, як характеристика особливостей педагогічної взаємодії поколінь, як засіб педагогізації навколишнього середовища.

В аспекті діяльності навчальних закладів педагогічна культура досліджується як сутнісна характеристика середовища, способу життя, особливостей педагогічної системи, як процес її руху до нового якісного стану.

В індивідуально-особистісному аспекті вона розглядається як вияв сутнісних властивостей особистості, професійної діяльності і спілкування педагога.

Культура професійно-педагогічної поведінки передбачає, що за всіх обставин комунікації та взаємодії викладач дотримується норм моралі та педагогічної етики, виявляє гідність, доброзичливість, витримку, культуру спілкування, такт.

Гуманна педагогічна позиція, психолого-педагогічна компетентність, авторизація педагогічного досвіду концептуалізує професійну поведінку педагога, надає йому власного педагогічного стилю.

Окрім того, що викладач володіє особистісними рисами високої якості, інформаційною та педагогічною культурою, у його діяльності важливе значення мають *знання та вміння*.

Студент має сприйматись викладачем як суб'єкт навчання, їх взаємодія має будуватись на основі діалогічного підходу, що забезпечує суб'єкт-суб'єктні стосунки, які ґрунтуються на рівності позицій, повазі та довірі до студента як свого партнера. Саме це дає змогу зрозуміти один одного і є найкращим способом взаємодії, а також допомагає задовольнити особисті потреби й інтереси всіх учасників навчального процесу. Сучасний викладач не має бути маніпулятором, тобто не намагатися підкоряти і контролювати волю слухачів

для досягнення власної мети; він має володіти протилежним до маніпуляції потенціалом – самоактуалізацією.

Мистецтво слова, що звучить, як частина сценічного мистецтва, надзвичайно важливе для викладача. Завжди слід пам'ятати, що слово – найважливіший і найвагоміший засіб впливу. Тому, якщо хочеш мати авторитет, то маєш досконало володіти мовою виразності. Слухачі мають «чути», що він говорить: вимагає чи просить, сміється чи жартує, наказує чи попереджає, радить чи забороняє, захоплюється чи засмучується, обурюється чи дивується, страждає чи соромиться, закликає чи розмірковує. Безліч почуттів і відтінків, які здатен висловити викладач, міцно входять у душу вихованців. Володіючи цим найтоншим інструментом – мистецтвом слова, легше оволодіти свідомістю аудиторії.

Мистецтво поведінки, рухів, жестів, міміки, інтонацій, яке спирається на рекомендації сценічного мистецтва, міститься в тому, щоб чітко і щиро, із врахуванням сприйняття слухачами, виразити себе, зробити якнайбільший вплив, повести їх за собою.

Відомо, що при спілкуванні переважає вербальний зв'язок між партнерами. Проте не слід применшувати значення невербального. Відомий німецький філософ І. Кант[27] сказав: «Рука – це видима частина мозку». Крім словесного мовлення, ми володіємо мовою тіла. Доведено, що людина словесно здобуває 35% інформації, а за допомогою тіла – 65 %. Нині описано і витлумачено більш як 1000 несловесних знаків і сигналів. Жести, міміку треба вміти контролювати. Непродумані рухи можуть відволікати слухача або ж виказувати приховані наміри. Так, під час народних заворушень у Литві, яка прагнула державного суверенітету й виходу із СРСР, на засіданні Верховної Ради президент М. Горбачов сказав: «Проблему з Литвою ми будемо розв'язувати демократичним шляхом!» - і при цьому вдарив кулаком по трибуні. Наступного дня у Вільнюс ввели війська. Так жест передав те, що не було сказано словами.

Заняття наукою – специфічний вид людської діяльності, суть якого – систематичний процес досліджень, спрямований на здобуття знань, що ґрунтуються на перевірених результатах. Основні ділові стосунки науковців, їх

[27] Іммануї́л Кант (нім. Immanuel Kant; 1724, Кенігсберг – 1804, Кенігсберг, Німеччина), німецький філософ, родоначальник німецької класичної філософії. У своїх численних роботах стверджував, зокрема, що умова пізнання – загальнозначимі апріорні форми, що упорядковують хаос відчуттів. Ідеї Бога, волі, безсмертя, недовідні теоретично, є, однак, постулатами «практичного розуму», необхідною передумовою моральності.

обов’язки і права визначені та установлені в законі України «Про наукову і науково-технічну діяльність» [26].

Етика науки – це галузь, що вивчає специфіку моральної регуляції в науковій сфері, а також зведення цінностей, норм і правил у цій галузі. Вона охоплює два кола проблем: перше пов'язане з регуляцією взаємовідносин всередині самого наукового співтовариства, а друге – між суспільством в цілому і наукою.

Наукова етика – у сучасній науці це сукупність офіційно опублікованих правил, порушення яких веде до адміністративного розгляду.

Вчений повинен додержуватися принципів наукової етики, щоб успішно займатися науковими дослідженнями. У науці як ідеал проголошується принцип, що перед обличчям істини всі дослідники рівні, що жодні минулі заслуги не беруться до уваги, якщо мова йде про наукові докази. Не менш важливим принципом наукового етосу є вимога наукової чесності при викладі результатів дослідження. Учений може помилятися, але не має права фальсифікувати результати, він може повторити вже зроблене відкриття, але не має права займатися плагіатом. Посилання як обов'язкова умова оформлення наукової монографії й статті покликані зафіксувати авторство тих або інших ідей і наукових текстів, і забезпечувати чітку селекцію вже відомого в науці й нових результатів. Існують детально розроблені правила про те, яким умовам повинні відповідати співавтори наукової статті. Нижче наведена витримка із правил, розроблених у Гарвардському Університеті.

Кожний, хто вказаний як автор, повинен внести суттєвий безпосередній інтелектуальний внесок у працю. Наприклад, повинен внести вклад у концепцію, дизайн і/чи інтерпретацію результатів. "Почесне" співавторство заборонене. Надання фінансування, технічної підтримки, пацієнтів або матеріалів, як би це не було важливо для роботи, само по собі не є достатнім внеском у роботу для того щоб стати співавтором. Кожен, хто вніс істотний вклад у роботу, повинен бути співавтором. Кожний, хто вніс менш значний внесок у роботу повинен бути перелічений у списку людей, яким виноситься подяка наприкінці статті.

Дані моральні принципи часто порушуються. У різних наукових співтовариствах може встановлюватися різна жорсткість санкцій за порушення етичних принципів науки. Зниження «якості знання» при порушенні етики науки веде до макулатурної науки, ідеологізації науки, і комерціалізації науки (у кого основна мета є гонка за фінансуванням). Одним з важелів контролю над

виконанням наукової етики є анонімне рецензування наукових статей, проектів і звітів.

Наукова етика – це не тільки адміністративні правила, але так само й сукупність моральних принципів, яких дотримуються вчені в науковій діяльності і які забезпечують функціонування науки [27-29]. Основні етичні принципи наукової діяльності, які визнаються більшістю вчених є такими:

- самоцінність істини;
- новизна наукового знання;
- свобода наукової творчості;
- відкритість наукових результатів;
- організований скептицизм.

До норм, що регулюють повсякденну наукову діяльність, належать:

- точне дотримання правил здобування та відбору даних, що діють в конкретній науковій дисципліні;
- надійна організація захисту та зберігання первинних даних. Ясне і повне документування всіх важливих результатів;
- осмислення неявних, аксіоматичним припущень. Пильне ставлення до спроб прийняти бажане за дійсне, викликаних особистою зацікавленістю або навіть причинами етичного характеру. Обережне ставлення до ймовірності неправильного тлумачення через методично обмежені можливості встановити об'єкт досліджень.

Норми, що регулюють стосунки між колегами і співробітниками:

- зобов'язання не перешкоджати науковій роботі конкурентів, шляхом, наприклад, затримки відгуків або передачі третій особі наукових результатів, здобутих за умови дотримання конфіденційності;
- активне сприяння науковому зростанню молодих учених;
- відкритість для критики і сумнівів, які висловлюються іншими вченими та колегами по роботі;
- уважна, об'єктивна і неупереджена оцінка роботи колег; не-упереджене ставлення до них.

До норм, що регулюють публікацію результатів відносять:

- обов'язкова публікація результатів роботи, що виконується за рахунок державних коштів (принцип загальнодоступності результатів фундаментальних досліджень);

- відповідне подання непідтверджених гіпотез і визнання помилок (принцип наукової культури, що допускає можливість помилки в науці);
- чесне визнання заслуг і належна оцінка внеску попередників, конкурентів і колег (принцип визнання заслуг).

Роберт Мертон[28] у своїх роботах із соціології науки створив чотири моральні принципи:

- колективізм – результати дослідження повинні бути відкриті для наукового співтовариства;
- універсалізм – оцінка будь-якої наукової ідеї або гіпотези повинна залежати тільки від її змісту й відповідності технічним стандартам наукової діяльності, а не від соціальних характеристик її автора, наприклад, його статусу;
- безкорисливість – при опублікуванні наукових результатів дослідник не повинен прагнути до одержання якоїсь особистої користі, крім задоволення від розв'язки проблеми;
- організований скептицизм – дослідники повинні критично ставитися як до власних ідей, так і до ідей, що висуваються їхніми колегами.

Основні принципи і вимоги наукової етики до науковця сформовані у Додатку В.

Висновок. Науково-педагогічна етика - це невід'ємна складова науки та освіти. Дотримання принципів науково-педагогічної етики забезпечує розвиток науки та освіти на основі межі та сприяє підвищенню моральних та етичних стандартів. Науковці та викладачі повинні відчувати відповідальність за свою роботу та діяти з урахуванням етичних принципів. Це допомагає зберегти довіру громадськості до науки та освіти, а також сприяє розвитку демократичного суспільства.

Загалом, принципи науково-педагогічної етики допомагають науковцям та викладачам вести свою роботу відповідно до моральних та етичних стандартів. Дотримання цих принципів є основою для розвитку науки та освіти, забезпечує повагу до прав людини та сприяє підвищенню якості наукових досліджень та педагогічної діяльності.

[28] Роберт Кінг Мертон (4 липня 1910– 23 лютого 2003) – американський соціолог, який вважається батьком-засновником сучасної соціології і одним з головних авторів підгалузі кримінології.Википедия site:wiki5.ru

Питання для самоконтролю:

1. Хто вперше розробив кодекс педагогічної етики і в чому його суть?
2. Що є предметом педагогічної етики?
3. Які елементи складають структуру моралі?
4. Назвіть основні показники педагогічного такту.
5. Назвіть можливі стилі спілкування викладач – студент.
6. Які етичні норми регулюють стосунки між науковцями?
7. Які етичні норми регулюють публікаційну діяльність науковців?

Завдання:

1. Підготувати доповідь (реферат) на тему: Етика наукової публікації. Вимога істинності та новизни. Плагіат. Норми цитування. Співавторство.
2. Знайти та ознайомитись із вимогами до оформлення наукової статті в журналі «Сучасний захист інформації», «Телекомунікаційні та інформаційні технології».

1.6. Етична філософія кібербезпеки

На сьогоднішній день провідні держави світу та суспільство в цілому все більшою мірою покладаються і залежать від безперешкодного функціонування п’ятого простору – *кіберпростору*, під яким розуміється сукупність взаємопов’язаних інформаційних ресурсів, програмного забезпечення, баз та банків даних, що обробляються в комп’ютерних мережах і пов’язаній з ними інфраструктурі, разом з об’єктами, що підпадають під їх контроль та управління. Захист інтересів держав та громадян в кіберпросторі стає життєво важливим завданням, яке перетворює безперешкодне використання ІТ-мереж на питання безпеки й оборони. Потенційна небезпека може загрожувати системам державного та військового управління, економіки та промисловості.

Україна інтегрована у світовий кіберпростір і зазнає різних загроз і негативних впливів, пов’язаних з його розвитком (зокрема від наслідків суперництва США і ЄС з РФ та КНР), що гостро актуалізує проблеми

кібербезпеки на загальнодержавному рівні. Це призводить до необхідності концептуального розуміння нової кібербезпекової реальності, впорядкування внутрішнього нормативно-правового поля, визначення повноважень відомств та організацій, задіяних у забезпеченні кібербезпеки держави і вирішення комплексу проблем, пов'язаних із розбудовою національної системи кібербезпеки. Найбільш ефективним шляхом вирішення зазначених питань є побудова національної моделі кібербезпеки та розробка першочергових напрямків діяльності державного та приватного секторів у сфері кібербезпеки [30].

Кібербезпека – це практична діяльність, спрямована на захист комп'ютерних систем і мереж від кібератак. Вона охоплює весь комплекс заходів – від керування паролями до інструментів комп'ютерної безпеки на основі технологій машинного навчання. Кібербезпека дає змогу надійно виконувати торговельні операції, спілкуватися та переглядати контент в Інтернеті.

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 [31].

Стратегія кібербезпеки здатна забезпечити надійний захист від атак, спрямованих на отримання доступу, зміну, видалення, знищення або вимагання конфіденційних даних компаній, організацій або окремих користувачів. Також кібербезпека здатна запобігати атакам, які спрямовані на відключення або порушення роботи систем та пристроїв [31].

Розвиток інформаційних технологій та мережі Інтернет призвели до виникнення ряду моральних проблем. В результаті функціонування кібербезпеки, як практичної діяльності кіберорганів та організацій що займаються кібербезпекою, сформувались етичні норми цієї діяльності, які називаються кіберетикою [32].

Кіберетика – це філософське вивчення етики, що стосується комп'ютерів, охоплює поведінку користувачів і те, що комп'ютери запрограмовані робити, та як це впливає на окремих людей і суспільство. Протягом багатьох років різні уряди ухвалювали нормативні акти, а організації визначали політику щодо кіберетики.

Основні положення, що розглядаються у кіберетиці:

- право інтелектуальної власності інформації у кіберпросторі;
- конфіденційність і доступність інформації, розміщеної в просторах Інтернету;

Більшості людей сьогодні при виконанні простих дій в Інтернеті стикаються з вірусами та векторами загроз, але знань недостатньо для того щоб убезпечити себе від них. Вони використовують комп'ютери, смартфони та мережі для інших справ, тому повинні довірити свою безпеку експертам. Однак необхідно розуміти, що експерти з кібербезпеки стикаються з особливими етичними проблемами, з якими інші можуть ніколи не мати справу.

Конфіденційність є ключовим етичним питанням у сфері кібербезпеки. Фахівці з безпеки за характером своєї професії бачать і обробляють особисту, приватну або конфіденційну інформацію, яка повинна зберігатися в суворій конфіденційності. У людей, які працюють у цих сферах, може виникнути спокуса розкрити будь-які соковиті плітки, які вони виявили під час запуску сканування вірусів на чиємусь жорсткому диску, але це може зруйнувати кар'єру чи особисте життя цієї людини. Фахівці з кібербезпеки повинні слідувати тому правилу, який назвали «кредо дворецького»: Дворецький ніколи нікому нічого не повинен розповідати [33].

Безпека - це ще одне етичне питання, яке може здатися зайвим, якщо говорити про професіонала з кіберзлочинності, але з іншог боку, якщо ми всі несемо відповідальність за дотримання відповідних процедур кібербезпеки у власному житті, то візьміть свій особистий рівень відповідальності та помножте його на 100 - це відповідальність за безпеку фахівця з кібербезпеки. Якщо більшість людей залишають свій комп'ютер без нагляду або будуть нехтувати виконанням запланованого оновлення, це може не бути великою проблемою, але для експерта з кібербезпеки це може бути серйозним етичним провалом, тому що на їхню відповідальність покладено 100 і більше комп’ютерів організації. Вони, як ніхто, зобов'язані зберігати пристрої, дані та мережі в безпеці.

Інший приклад. Працюючи в компанії, яка в основному робить хорошу роботу, дехто поводиться неетично, ведучи документацію тіньового бізнесу. Якщо викрасти електронну документацію тіньової практики бізнесу та надати її засобам масової інформації чи правоохоронним органам, можна пролити світло на такі правопорушення і зупинити їх. Це є доброю справою, або, принаймні, зроблена сумнівна справа, щоб досягти хорошого результату. Тоді людина, яка

це зробила, буде рахуватись як інформатор. Але чи виправдовує мета засоби? Чи це етично?

Відповідь, звичайно, залежить від деталей ситуації, а також від того, кому поставити запитання. Для багатьох людей Едвард Сноуден[29] є героєм, який виявив, що Агентство національної безпеки веде неетичне стеження за невинними американцями. Однією з головних причин, чому Сноуден вкрав секретні файли з Агентства і надав їх громадськості, є те, що він відчував, що агентство збирає занадто багато інформації про неправильних людей. Іншими словами, він вважав, що Агенство порушує приватне життя законослухняних американців без вагомих на те причин. Той факт, що йому довелося вкрасти документацію цих дій, щоб надати її громадськості, майже повністю не має сенсу. Для інших він злочинець (ця частина не підлягає сумніву) і зрадник, який поставив під загрозу життя розвідників, які працюють на США і їх союзників, розкриваючи секретну інформацію про підпільні операції. Чи поводився він етично?

Проблеми конфіденційності з питаннями кібербезпеки знаходяться в складних відносинах. Кібербезпека покликана захистити нас від таких загроз, як програми-вимагачі і крадіжка особистих даних - це дві форми злому, які залежать від глибокого порушення конфіденційності користувача. Подумайте про масштаби резонансних порушень, які сталися нещодавно: 70 мільйонів транзакцій з кредитними картками Target, зареєстрованих злодіями, 87 мільйонів записів користувачів Facebook, скомпрометованих Cambridge Analytica[30], 143 мільйони кредитних записів Equifax[31], вкрадених невідомими сторонами [34].

---

[29] Е́двард Джо́зеф Сно́уден (англ. Edward Joseph Snowden; народився 21 червня 1983, Елізабет-Сіті, штат Північна Кароліна) – американський програміст, системний адміністратор, колишній працівник ЦРУ та АНБ США. У червні 2013 року передав газетам The Guardian і The Washington Post інформацію про стеження Агентством національної безпеки США за інформаційними системами багатьох країн світу, що спричинило низку міжнародних скандалів. Сноуден був заочно звинувачений у шпигунстві і оголошений в міжнародний розшук.

[30] Cambridge Analytica – приватна англійська компанія, яка використовує технології глибинного аналізу даних (зокрема, даних соцмереж) для розробки стратегічної комунікації в ході виборчих кампаній в Інтернеті. Вона виникла у 2013 році як «дочірнє підприємство» британської компанії SCL Group для участі в політичних кампаніях США. Компанія частково належить підприємцю Роберту Мерсеру. Cambridge Analytica займається збором даних про користувачів Інтернету і соцмереж, складанням їх психологічних портретів і розробкою персоналізованої реклами. Алгоритми, що лежать в основі технологій, які використовує компанія Cambridge Analytica, значною мірою були розроблені Міхалом Косинським, психологом польського походження, з Кембриджського університету і Стенфордської вищої школи бізнесу

[31] Equifax - американське бюро кредитної історії, збирає інформацію про більш ніж 800 мільйонів фізичних осіб і більш ніж на 88 мільйонів компаній по всьому світу. Засноване в 1899 році, розташована в Атланті, штат Джорджія. Є одним з трьох найбільших кредитних агентств в США, поряд з Experian і TransUnion (разом їх називають "великою трійкою"). Річний дохід Equifax становить 3,1 мільярда доларів США, в компанії працює понад 9 тисяч співробітників у 14 країнах.

Організації, які володіють особистою інформацією про своїх користувачів, несуть етичну відповідальність за захист цієї інформації від хакерів. На жаль, у багатьох гучних порушеннях даних організацій, які були зламані, були принаймні частково винні самі організації. Наприклад, у випадку з Equifax, спочатку фірма була зламана через веб-портал скарг споживачів на сайті компанії. Нападники використовували широко відому уразливість через веб-портал скарг споживачів на сайті компанії, через яку Equifax вже давно повинна була бути зламаною. Однак внутрішні процеси компанії для забезпечення безпеки інформації були недостатніми або їх не дотримувалися, через що вразливість залишалася неліквідованою і залишала двері широко відкритими для хакерів щоб зайнятися крадіжкою.

Часто кажуть, що деякі цінності, пов'язані з кібербезпекою, суперечать одна одній. Найбільш часто згадуваний конфлікт – це конфлікт між безпекою та конфіденційністю, але це, звичайно, не єдиний можливий конфлікт цінностей у сфері кібербезпеки. Технологія кібербезпеки, спрямована на захист конфіденційності, наприклад шифрування, загалом узгоджується з правами людини. Загроза правам людини зазвичай полягає не в кібербезпеці, а в недостатній кібербезпеці або її відсутності. Однак можуть бути випадки, коли технологія кібербезпеки для захисту конфіденційності є одночасно засобом захисту конфіденційності та загрозою. Технології кібербезпеки, такі як шифрування, природно супроводжуються автентифікацією (що відрізняє тих, хто має право отримати незашифровану інформацію, від решти). Автентифікація передбачає сертифікацію та керування обліковими даними. Це вимагає збору інформації про окремих осіб, що може призвести до порушення конфіденційності користувачів.

Моніторинг веб-трафіку та боротьба із кіберзлочинністю – знаходяться в більш прямому конфлікті з правами людини. Моніторинг пов'язаний із стеженням, а стеження передбачає погрози цензури (що може бути порушенням права людини на свободу слова) та підслуховування (що може бути порушенням права людини на належну судову процедуру).

Крім того, моніторинг пов'язаний із профілюванням[32]. Профілювання «може використовуватися поліцією або службами безпеки для пошуку злочинців або терористів; аеропортами, щоб вирішити, кого перевіряти

[32] Профілювання – надавання правильного, потрібного профілю чому-небудь (людині, дорозі, площадці, деталі, заготовці і т. ін.)

ретельніше» [33]. Таким чином, профілювання пов'язане з потенційними порушеннями прав людини на боротьбу з дискримінацією, оскільки під час профілювання до людей підходять, засуджують або поводяться певним чином, тому що вони мають характеристики, які відповідають певному профілю та які пов'язані з деякими іншими рисами (тобто ознаки, відмінні від тих, за якими вони ідентифікуються як належні до профілю). Основним етичним питанням профілювання є не конфіденційність, хоча особиста інформація може використовуватися для створення профілів. Справа в тому, що профілювання може завдати різного роду незаслуженої шкоди людям, від неприємностей до фальшивих звинувачень і навіть, у крайніх випадках, до ув'язнення невинних людей. Це відбувається тому, що під час профілювання «узагальнення робиться на основі обмеженої інформації про особу».

Статистична дискримінація, пов'язана з будь-якою формою профілювання, суперечить праву людини на недискримінацію лише тоді, коли профілювання стосується конкретних (як правило, захищених законом) категорій. Фундаментальне право на недискримінацію стосується заборони дискримінації в контексті професії чи зайнятості, надання товарів і послуг або в інших важливих сферах повсякденного життя, таких як житло, соціальне забезпечення чи охорона здоров'я. Захист права людини від дискримінації є однією з цілей регулювання захисту даних і закріплено в Розділі III Хартії ЄС, який включає гендерну рівність (стаття 23) і також забороняє «будь-яку дискримінацію за будь-якою ознакою, такою як стать, раса, колір шкіри, етнічне чи соціальне походження, генетичні особливості, мова, релігія чи переконання, політичні або будь-які іншу думку, належність до національної меншини, майновий стан, народження, інвалідність, вік чи сексуальну орієнтацію» (ст. 21) [35].

Технології кібербезпеки, які захищають людей від кіберзлочинності, можуть суперечити правам людини. Більшість дослідників визначають кіберзлочинність так, щоб вона включала чотири різні широкі категорії злочинів: кіберзлочинство, кібервандалізм, кіберпіратство та комп'ютерне шахрайство [30, 33-36]. Перший стосується отримання несанкціонованого доступу до даних та інформаційних систем, другий – зриву процесів і пошкодження даних, третій – відтворення та розповсюдження програмного забезпечення чи контенту, що порушує інтелектуальну власність, а четвертий – спотворення особи чи інформації з метою обману для особистих цілей.

Таким чином, кібербезпека сама по собі не є справжньою етичною цінністю, тому ми можемо поставити наступне запитання про те, як аналізувати етичні проблеми, які виникають під час забезпечення кібербезпеки.

Як збалансувати необхідність бути в безпеці з необхідністю захисту нашої конфіденційності?

Як визначити ступінь етичної відповідальності організації за захист нашої інформації або повагу до нашої конфіденційності та як притягнути їх до відповідальності?

Перший крок, який нам потрібно зробити, - це оцінити конфіденційність як гідну самоціль. Уявлення про те, що люди мають право на приватність, випливає з етичної ідеї про те, що люди мають внутрішню цінність і гідність. Істоти з гідністю мають право на приватне життя, як особисто, так і в Інтернеті. Поводитися або вірити в інше порушило б наші найглибші етичні принципи. Це відправна точка для набору етичних дебатів, які ми повинні мати. Можливо, ми ніколи не прийдемо до рішення, яке сподобається всім, але принаймні ми будемо задавати правильні питання і рухатися в правильному напрямку: більша безпека, безпека та конфіденційність для всіх нас.

Спостерігач за інтернетом під час інформаційної війни створює загрози праву на приватне життя та свободу слова підозрюваних і фактичних жертв (що може бути особливо актуальним для уряду у вигнанні). Ці загрози викликані пасивним моніторингом імовірних жертв-моніторів (без згоди) і подальшим збором даних із уражених комп'ютерів (за згодою). З точки зору принципового підходу, інформована згода та повідомлення виконують обов'язок поваги осіб. З точки зору підходу, що ґрунтується на правах, їх можна розглядати як спосіб збалансувати (у сенсі системи стримувань і противаг) ризик для конфіденційності жертв, спричинений моніторингом. Можна стверджувати, що інформована згода зменшує вразливість, до якої наражає суб'єкта права порушення конфіденційності та стеження. Крім того, з точки зору принципів, заходи безпеки, вжиті під час зберігання та обробки даних з комп'ютерів жертви (наприклад, шифрування, анонімізація тощо), виконують обов'язок благодійності (що включає нешкідливість як зменшення ризику). З точки зору підходу до прав людини, їх можна розглядати як спосіб збалансувати (у сенсі стримувань і противаг) підвищений ризик для конфіденційності та інформаційного самовизначення всіх інших осіб, яким дані на заражених комп'ютерах може ідентифікувати.

Розгляд етичних проблем у кібербезпеці ще не набрав закінченого вигляду. Наукова спільнота для досліджень і обміну результатами продовжує обговорювати етичні проблеми на різних міжнародних майданчиках. Багато світових організацій представляють значний інтерес до кіберетичних дебатів.

Міжнародна федерація з обробки інформації (ІФІП) – всесвітня організація для дослідників і фахівців, що працюють в області інформаційних і комунікаційних технологій (ІКТ). Створена в 1960 році під егідою ЮНЕСКО.

Асоціація обчислювальних машин - (англ. Association for Computing Machinery, (ACM)) – найстарша і найбільша міжнародна організація в галузі комп'ютерних наук. Є неприбутковою організацією. Об'єднує близько 100 000 спеціалістів. Штаб-квартира розташована у Нью-Йорку. Щорічно асоціація присуджує Премію Тюрінга і нагороду імені Ґрейс Мюррей Гоппер. До числа нагород від асоціації також входять Премія Геделя, Премія Дейкстри, Премія Кнута, Премія Гордона Белла і Премія Канеллакіса.

Електронний інформаційний центр конфіденційності (EPIC) є незалежним некомерційним дослідницьким центром у Вашингтоні, округ Колумбія. Місія EPIC - зосередити увагу громадськості на конфіденційності, що пов’язана з питаннями прав людини. EPIC працює для захисту конфіденційності, свободи самовираження та демократичних цінностей, а також сприяття громадському голосу при прийнятті рішень щодо майбутнього Інтернету.

Electronic Frontier Foundation (EFF) – міжнародна некомерційна юридична організація, розташована в США, що спеціалізується на захисті громадянських прав у галузі цифрового права.

Висновок. Етика кібербезпеки є важливим аспектом сучасного життя, оскільки комп'ютерні технології та Інтернет використовуються в усіх сферах нашого життя. Захист інформації та безпека в мережі стали основними проблемами, які потребують уваги та дій з боку користувачів. Дотримання етичних принципів кібербезпеки, таких як захист конфіденційної інформації, відповідальне використання Інтернету та комп'ютерів, використання сильних паролів та методів аутентифікації та забезпечення безпеки в мережі, можуть допомогти зберегти безпеку та конфіденційність даних вмережі. Крім того, дотримання етичних принципів кібербезпеки є необхідним для забезпечення довіри між користувачами та інтернет-сервісами, що є ключовим фактором розвитку електронної комерції та інших онлайн-сфер.

На сьогоднішній день кібербезпека є серйозним питанням, яке стає все більш актуальним в суспільстві. Зокрема, під час пандемії COVID-19 багато людей почали використовувати Інтернет для роботи та освіти, що збільшило кількість потенційних загроз для кібербезпеки. Тому важливо, щоб кожен користувач Інтернету дотримувався етичних принципів кібербезпеки та був свідомим про свої дії в мережі.

Дотримання етичних принципів кібербезпеки, таких як захист конфіденційної інформації, відповідальне використання Інтернету та комп'ютерів, використання сильних паролів та методів аутентифікації та забезпечення безпеки в мережі, є важливим для збереження безпеки та конфіденційності даних в мережі.

Питання для самоконтролю:

1. Для чого організовується кібербезпека в державі?
2. Що є об’єктами кібербезпеки?
3. В чому полягає стратегія кібербезпеки?
4. Які проблеми розглядає кіберетика, де і хто їх намагається вирішити?
5. У чому суть філософського значення кіберетики?

Завдання:

Приклад. Монітор інформаційної війни: ви розслідуєте шкідливий ботнет, жертвами якого стали іноземні посольства десятків країн, тибетський уряд у вигнанні та міжнаціональні консалтингові фірми. Ви починаєте своє дослідження з перегляду даних, зібраних шляхом пасивного моніторингу ймовірних мереж-жертв, які підтверджують вторгнення та ідентифікують шкідливе програмне забезпечення. Ви збираєте більше даних із скомпрометованих комп’ютерів за згодою власників, відстежуєте інфраструктуру командування та контролю (C&C) достатньо, щоб зрозуміти дії зловмисників і ввімкнути сповіщення заражених сторін у відповідний час, співпрацюєте з державними органами в різних юрисдикціях щоб зруйнувати інфраструктуру C&C зловмисника, а також безпечно зберігати й обробляти дані.

Завдання: визначити як класифікувати дії?

Розділ 2
ЕТИКА ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ В УПРАВЛІННІ КІБЕРБЕЗПЕКОЮ

2.1. Види та загальні принципи професійної і корпоративної етики в кібербезпеці та їх сучасне функціонування

Через поглиблення професіоналізації праці перед спеціалістами різноманітних напрямів все частіше виникають моральні колізії, вирішити які неможливо, спираючись тільки на професійні знання. Більше того, професійне захоплення, позбавлене моральних критеріїв та цінностей, може бути небезпечним як для самої людини, так і для оточуючих, а в більш широких масштабах - і для суспільства загалом. Тому проблеми професійної етики зовсім не зайвий додаток до професійної освіти.

Професійна етика – це кодекс правил, що визначає поведінку спеціаліста у службовій обстановці, а також перелік норм, які відповідають існуючим законам та відомчим нормативним документам, професійним знанням, стосункам у колективі, глибокому усвідомленню моральної відповідальності за виконання професійних обов'язків. Професійна етика, крім того, це прикладна соціально-філософська дисципліна, яка вивчає походження, сутність, специфіку, суспільні функції морально-професійних норм і стосунків, закономірності їх розвитку на різних історичних етапах.

Крім особливостей кожної професії, в кожній організації і навіть у кожному структурному підрозділі кожної організації існують свої специфічні умови виконання функціональних обов’язків, умови взаємовідносин у колективі.

Розвиток корпоративної культури завжди мав головне завдання – згуртування колективу для ефективного досягнення необхідних результатів.

Корпоративна етика компанії будується на спільних цінностях, традиціях і нормах поведінки співробітників. Її базу складають [37]:

- цінності компанії, які розділяє кожен співробітник;
- дотримання загальної місії компанії;
- віра в успіх компанії;
- продуктивна співпраця між працівниками, що дозволяє досягати спільних цілей;

- кар'єрний розвиток: тренінги, курси, підвищення кваліфікації;
- мотивація, оцінка роботи, винагорода;
- норми ділової поведінки, стиль одягу.

Про корпоративну етику почали говорити з початком домінування в різних галузях господарської і соціальної діяльності великих компаній з чітким поділом видів на напрямкі трудової діяльності. З цієї точки зору метою корпоративної етики можна вважати не збереження високих стандартів професії, а саме формування єдиного корпоративного духу в компанії.

Корпоративна етика - це сукупність етичних правил, що містяться в документах, прийнятих добровільно представниками будь-якої професії, галузі, громадського об´єднання й обов´язкові для виконання особами, що є членами професійного, галузевого чи іншого локального об´єднання, що прийняла цей документ. Сукупність норм поводження підприємця, сукупність вимог, що їх культурне суспільство пропонує дотримуватися у спілкуванні з людьми, вимог, невід'ємних від усталеного образу ділової людини називається діловою етикою. Варто виділити такі принципи ділових взаємин: воля, терпимість, діловий обов'язок. Основний постулат етики кожної серйозної компанії – «прибуток понад усе, але честь понад прибутком».

Дотримання етики в компанії несе для неї ряд вагомих переваг, які вигідно виділяють компанію серед інших [37].

1. Залучення і відповідальність співробітників. Корпоративна етика об'єднує та згуртовує колектив. Її наявність дозволяє створити команду однодумців з однаковими цілями і місією.

2. Повага всередині колективу. Традиції стають основою шанобливого ставлення один до одного. А в такій атмосфері набагато легше працювати над спільними завданнями і досягати потрібних результатів.

3. Створення позитивного іміджу компанії. У сучасному світі, коли компаній стає все більше, мати позитивний імідж – не привілей, а необхідність. Це допоможе бізнесу не тільки залучити інвесторів, але і буде гарантією якості ваших послуг серед партнерів.

4. Збереження лояльності клієнтів. Компанія, в якій врегульовані всі процеси і чітко простежується порядок в роботі, заслуговує на більшу довіру клієнтів.

5. Вигідне розташування на ринку. Фахівці, які знають собі ціну, не працюють в компаніях-одноденках. Вони обирають перевірені часом організації,

які мають свої традиції і правила. Таким чином, компанія підвищує свій бренд роботодавця в очах фахівців.

6. Корпоративна етика як частина адаптації. Новачки, які тільки прийшли в компанію, легше переносять період онбординга, якщо мають загальне уявлення про діяльність компанії і її процесах. Перелік норм і правил позбавляє нового співробітника від зайвих питань і відразу дає зрозуміти, підходить йому компанія чи ні.

7. Рішення конфліктів. Правила корпоративної етики допомагають вирішувати конфлікти всередині колективу. При будь-якій суперечливій ситуації, ви можете звернутися до переліку правил і грамотно залагодити розбіжності.

Спільним з професійною етикою є те, що в основі об'єднуючої ідеології лежать моральні цінності, орієнтуючись на які корпорація могла б виправдати своє існування перед суспільством. З цієї точки зору, з метою провести більш чітке розходження між професійною і корпоративною етикою, треба розглядати область, близьку до науки, але, тим не менш, складову самостійної сфери соціальної практики – академічну етику, яку можна вважати класичним зразком складної сучасної корпорації. При цьому, співтовариство професіоналів можна при бажанні розглядати як корпорацію, але сенс і труднощі корпоративного регулювання полягають у тому, що його суб'єктом виступає не колегія фахівців, а спільнота однодумців, в якому трудяться люди різних професій, статусів та інтересів.

Завдання професійної етики в тому, щоб вивчити складний процес віддзеркалення професійних стосунків у моральній свідомості, у морально-професійних нормах, провести чітку межу між морально-професійними явищами і явищами професійної майстерності, вивчити суспільні завдання, цілі професії і їх значущість у соціальному прогресі, саме цим сприяючи їх успішному виконанню [7].

Професійна етика покликана дати теоретичне обґрунтування сутності трансформації загальних норм і принципів моралі до специфічних умов професійної діяльності людей відповідно до уявлень про професійний обов'язок, благо, добро і зло, справедливість, совість, честь та інші моральні цінності.

Види професійної етики - це ті специфічні особливості професійної діяльності, які спрямовані безпосередньо на людину в тих чи інших умовах його життя і діяльності в суспільстві.

Основними видами професійної етики є:

- лікарська етика,
- педагогічна етика,
- етика вченого,
- актора,
- художника,
- підприємця,
- журналіста,
- інженера і т.д.

Кожна професія має свою власну мораль. Професія формує у її носіїв не тільки професійні навики, але і певні риси особи і відношення до змісту своєї діяльності. Професійна діяльність утворює складну систему взаємозумовлених моральних стосунків. До цієї системи належать стосунки, що вивчаються професійною етикою:

- ставлення спеціалістів до об'єкта праці;
- стосунки спеціаліста з колегами;
- ставлення спеціаліста до суспільства.

Практичне застосування у країнах, де існують громадські органи та механізми підтримання стандартів діяльності окремих професій, порушення професійної етики, після їх розгляду спеціальними комітетами, можуть бути підставою для позбавлення особи ліцензії на право практикувати в рамках даної професії.

Соціальна відповідальність – це соціальне явище, що являє собою добровільне та свідоме виконання, використання і дотримання суб’єктами суспільних відносин, приписів, соціальних і моральних норм, а у випадку їхнього порушення – застосування до порушника заходів впливу, передбачених цими нормами.

Це волевиявлення, яке визначається певною поведінкою щодо дотримання усвідомлених обмежень та соціальних норм, гарантує безпеку та прогресивний розвиток, забезпечує узгодження інтересів суб’єктів, задіяних у суспільних відносинах та управлінні ними.

У залежності від видів соціальних норм виділяють такі різновиди соціальної відповідальності: моральна, релігійна, дисциплінарна, політична, правова (юридична) тощо.

Моральна відповідальність настає у випадку порушення традицій, звичаїв, норм культури та естетичних норм. Вона відображається у суспільному осуді та соціальному відмежуванні від суб'єкта, що порушуючи ухиляється від виконання норми поведінки.

Політична відповідальність настає при порушенні норм, дотримання яких покладається суспільством на публічного політика.

Корпоративна відповідальність настає у випадку порушення корпоративних правил, які прийняті певною соціальною структурою та не мають правового значення.

Релігійна відповідальність засновується на нормах, що регламентують порядок відправлення релігійних культів та на вірі у Бога.

Всі згадані вище види соціальної відповідальності мають пасивний характер, оскільки негативна реакція з боку суспільства у цих випадках не передбачає примусового впливу на порушника норм.

Правова відповідальність настає у випадку порушення норм державно-організаційного права. Вона має активний характер, оскільки передбачає активний психологічний вплив на порушника аж до застосування примусового фізичного впливу.

Корпоративний інтерес - оскільки ефективне функціонування корпорації, її виживання залежить від перевищення доходів над витратами, то головний корпоративний інтерес полягає в максимізації прибутку. Разом з тим безпосереднє вираження економічного інтересу має різну визначеність, втілюючись в поточних, середньострокових і стратегічних цілях (наприклад розширення ринку збуту, технічне переозброєння, збереження робочих місць, економічне зростання і т.д.). Оскільки реалізація економічного інтересу як максимізації прибутку вимагає нововведень як найважливішого засобу виживання корпорації, то необхідною умовою її розвитку є новаторство.

Будь-яка корпорація в ринковій економіці є товаровиробником і в цій якості зацікавлена в максимізації ціни, по якій її товари продаються на ринку. Однак вільна конкуренція та зіткнення корпоративного інтересу з інтересами споживачів призводить до гнучкого ціноутворення, до швидкої і безпосередньої реакції ціни на переваги споживача і в кінцевому рахунку утворення рівноважної ціни.

З цього випливає, що поняття соціальна відповідальність та корпоративний інтерес на практиці є протилежними, бо головною метою кожної

компанії є збільшення прибутку, і через це часто компанії забувають про соціальну відповідальність. Така ситуація є проблемою сьогодення, тому кожна компанія повинна вміти поєднувати ці два поняття в своїй роботі для гармонійного розвитку суспільства та балансу економіки, застосовуючи норми суспільної моралі та етики.

Новому напрямку професійної діяльності, який сформувався останніми десятиліттями завдяки розвитку і застосуванню інформаційних технологій та створенню кіберпростору, теж притаманні етичні професійні проблеми, які існують також у інших професіях, але із своїми особливостями, які розглянуті у Розділі 1 (п.1.3 – п.1.6). Для їх вирішення та регулювання професійної діяльності загалом а також в організаціях кібербезпеки на основі суспільної моралі формується і особливий вид – кіберетика (Розділ 1, п. 1.7).

Кіберетика – це кодекс відповідальної поведінки при використанні технологій [38]. Так само, як у нас є правила особистої взаємодії з людьми, існують рекомендації, яких слід дотримуватися, коли ми знаходимося в кіберпросторі. Як кібер-громадяни, ми несемо відповідальність за дотримання стандартів етичної поведінки, щоб допомогти зберегти Інтернет безпечним для всіх.

Організаційна політика кіберетики допомагає гарантувати організації те, що кожен, хто пов'язаний із організацією, буде виконувати етичні корпоративні вимоги щодо забезпечення безпеки інформації. Створюючи організаційну політику кіберетики, необхідно пам'ятати наступне:

- будьте чіткими щодо того, що очікується від співробітників та інших осіб, пов'язаних з організацією;
- переконайтеся, що всі розуміють наслідки порушення політики;
- переконайтеся, що політика кіберетики регулярно переглядається та оновлюється.

Для врахування вимог суспільної моралі при плануванні організаційних заходів забезпечення захисту інформації необхідно розглядати наступні питання:

- інтелектуальна власність;
- безпека та захист даних;
- кібербезпека;
- соціальні мережі;
- електронна пошта та зв'язок;

- використання комп'ютера та прийнятне використання ресурсів компанії.

Організаційні та технічні засоби забезпечення безпеки у будь-якій сфері діяльності людини не здатні забезпечити 100% захист системи в цілому та людської ланки зокрема. У кіберпросторі, де атаки можна очікувати невідомо коли і щосекунди, важливим є постійний контроль за станом безпеки інформації.

В Законі України «про основні засади забезпечення кібербезпеки України» зазначено, що *«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» [40].

Кібербезпека – це практика захисту комп'ютерних систем і мереж від несанкціонованого доступу або крадіжки. Кіберзлочинці можуть використовувати різноманітні методи для отримання доступу до систем, включаючи віруси, фішингові шахрайства та соціальну інженерію.

Коли справа доходить до кібербезпеки, необхідно мати на увазі, що профілактика завжди краще, ніж лікування. Легше запобігти атаці в першу чергу, ніж фіксувати пошкодження постфактум. Година профілактики вартує місяців а іноді і років лікування. Це означає, що краще вжити заходів для запобігання нападу, ніж усувати пошкодження постфактум.

Якщо ви вирішили продовжити кар'єру професіонала з кібербезпеки, ви повинні враховувати етику при використанні рішень безпеки, які передбачають адміністративний доступ до особистих пристроїв співробітників.

Якщо ви приєдналися до цієї професії, вам важливо мати всебічне розуміння всіх питань кіберетики, пов'язаних з IT, і зробити ці практики природною частиною вашої робочої поведінки. Це особливо важливо, якщо ви фахівець з кібербезпеки, який працює в такій галузі, як охорона здоров'я, враховуючи чутливий характер даних про здоров'я, які можуть бути вразливими до хакерів та інших цифрових загроз.

В останній час особливо важливим є безпека критичної інфраструктури, яка включає важливі сфери діяльності, що впливають на людину, суспільство, державу. Фахівці з кібербезпеки, маючи доступ згідно своїх обов’язків до конфіденційної інформації, яка часто включає особисті персональні дані (у сфері

охорони здоров’я), цінної корпоративної інформації організації (банківська таємниця, …), повинні вести себе етично і доводити своїм керівникам своїми діями, що вони гідні нагляду за цінною інформацією. На практиці це не так просто, через відсутність регулювання у більшості випадків.

ІТ-спеціалісти у своїх ролях захисників даних компанії бачать усе. Сюди входить велика кількість конфіденційної інформації щодо особистого життя співробітників, спілкування між клієнтами та персоналом відділу продажів або облікового запису, медичне страхування та медичні записи, нарахування заробітної плати та багато іншого.

Окрім загальної ввічливості, яка диктує ІТ-персоналу зберігати те, що вони бачать для себе, існують також більш конкретні причини для збереження конфіденційності даних та інформації. Ці причини варіюються від базової довіри до надзвичайно важливих юридичних питань. Деякі порушення безпеки можуть серйозно поставити під загрозу безпеку та добробут клієнта, здатність бізнесу функціонувати або навіть загрозу суспільству і держави в цілому.

Саме тому спочатку у критичних інфраструктурах почав формуватися напрям “культура безпеки”. Програмними документами ООН ще з 2002 р. (http://www.un.org/ru/documents/decl_conv/conventions/elements.shtml) визначається, що виникла потреба в глобальній культурі кібербезпеки, яка буде вимагати від усіх урахування наступних дев'яти взаємодоповнюючих елементів:

1) поінформованість;

2) відповідальність;

3) реагування;

4) етика;

5) демократія;

6) оцінка ризику;

7) проектування і впровадження засобів забезпечення безпеки;

8) управління забезпеченням безпеки;

9) переоцінка.

Відповідно, головними напрямами розробки питань з кібербезпеки вважаються інформаційна безпека, безпека мережі, безпека Інтернету та захист критичних інфраструктур, а також захист різного роду даних. Ці елементи відносяться до усіх можливих напрямів кібербезпеки – інформаційних (1, 6 і 9), технічних (3 і 7), організаційних (5 і 8) і психологічних (2 і 4).

Фахівця кібербезпеки можуть покликати допомогти відділу кадрів організації перевірити потенційних співробітників, надати їм допомогу у забезпеченні безпеки інформації на робочих місцях. Це означає, що ви повинні бути знайомі з азами в галузі кібербезпеки з нуля, щоб нові працівники негайно прийняли етичні умови та вимоги.

Сьогодні прийнято говорити про професійну етику лікаря, педагога, журналіста, депутата, судді. Є відповідні етичні кодекси в бізнесі, у військових, у сфері торгівлі. Окремим напрямком сформувалась етика управлінця (менеджера, керівника), яка стосується також мнеджера кібербезпеки.

Етичні принципи керівника (управлінця):

- випробовувати кожного нового працівника, перш ніж прийняти його на роботу;
- вивчати і добре знати підлеглих, правильно оцінювати їхні позитивні риси і недоліки;
- допомагати підлеглим освоювати доручену справу, нові і суміжні професії;
- час від часу переглядати систему оплати та стимулювання праці;
- ефективно використовувати професійні вміння та здібності працівників з творчими нахилами, особливо раціоналізаторів і винахідників;
- створювати у колективі нормальну робочу атмосферу, намагатися, щоб кожен працівник почував себе на своєму місці;
- уміти осміхатися, підтримувати гарний настрій;
- критично оцінювати результати своєї роботи і роботи підлеглих, а також умови, у яких вона виконується;
- не порушувати закони, особливо коли це стосується фінансів;
- вміти обґрунтовувати ціну вироблюваної продукції, доходи своїх працівників, інші показники роботи колективу;
- не бути дріб'язковим, не шкодувати грошей на суспільне значущі, доброчинні цілі; не боятися конфліктів у колективі, вміти їх залагоджувати;
- вірити своїм працівникам на слово, довіряти їм, але водночас і пам'ятати, що не всі люди чесні, порядні;
- не забувати, що поруч діють конкуренти і вони можуть, у тому числі і через його працівників, вивідати службову, виробничу та комерційну таємницю;

- уникати справ з непорядними людьми, звільняти працівників, які порушили чесне слово;
- мати гарного і надійного секретаря, помічника.

Таким чином, в сучасному світі, в якому Інтернет відіграє все більш важливу роль, кібербезпека є однією з найбільш актуальних тем. Інформаційні технології та мережі є невід'ємною частиною бізнесу, індустрії та суспільства загалом. Однак, разом зі зростанням залежності від цифрових технологій зростає і кількість загроз, пов'язаних з кібербезпекою.

Корпоративна етика в кібербезпеці стає все більш важливою для підприємств та організацій, які прагнуть зберегти свої дані та захистити свою репутацію. Основними принципами корпоративної етики в кібербезпеці є:

Захист конфіденційної інформації та даних. Корпорації повинні захищати конфіденційну інформацію та дані від несанкціонованого доступу, викрадення та втрати. Крім того, корпорації повинні дотримуватися відповідних правових норм при регуляці моральної поведінки всередині компанії.

Повага до прав інших осіб. Корпорації повинні дотримуватися законів та стандартів, які встановлені для захисту прав інших осіб, включаючи захист приватності та інтелектуальної власності.

Відповідальність за власні дії. Співробітники корпорації повинні розуміти, що їх дії в Інтернеті можуть мати вплив на підприємство та його репутацію. Вони повинні бути відповідальними за свої дії та використовувати Інтернет та інформаційні технології з метою досягнення етичних цілей.

Прозорість та чесність. Корпорації повинні бути відкритими та чесними у своїх діях, включаючи дії, пов'язані з кібербезпекою. Вони повинні інформувати своїх клієнтів та співробітників про заходи, які вони приймають для захисту їх даних та інформації.

Навчання та освіта. Корпорації повинні забезпечувати своїх співробітників навчання та освіту з питань кібербезпеки. Вони повинні забезпечити своїх працівників необхідними знаннями та навичками, щоб вони могли розуміти загрози, які виникають при виконанні функціональних обовязків фахівцями кібербезпеки.

 *Питання для самоконтролю*:

1. У чому суть професійної етики?

2. У чому суть корпоративної етики?
3. В чому різниця між професійною та корпоративною етикою?
4. Як впливає суспільна мораль на формування етичних відносин у колективах?
5. В чому особливість кіберетики?

Завдання:

1. Визначити проблеми корпоративної етики Ощадбанку.

2.2. Професійна інформаційна і цифрова етика кібербезпеки

Людська цивілізація в процесі свого розвитку пройшла кілька етапів, на кожному з яких рівень життєдіяльності як окремих людей, так і спільнот залежав від їхньої поінформованості та здатності ефективно опрацьовувати дані. Етапи створення нових засобів і методів опрацювання даних, що спричинили суттєві зміни в суспільстві, тобто змінили спосіб виробництва, стиль життя, систему цінностей, називають інформаційними революціями. Інформаційні революції спричинили поетапний перехід від аграрного суспільства до інформаційного, де інтелект і знання є засобом і продуктом виробництва (рис. 2.1).

Рис. 2.1. Етапи розвитку суспільства

Про численні успіхи інформатики написані гори книг. Особливо вражаючим є факт виявлення фахівцями якогось ключа до розуміння мислення людини. Тим часом розвиток інформатики вселяє не тільки оптимізм, але і тривогу. Збої в інформаційних системах загрожують глобальними лихами. Віртуально-образні світи комп'ютерів викликають психічні захворювання у

частини користувачів. Інтернет взагалі став важкоконтрольованою системою. Інформатика - це не тільки вражаюче досягнення наукового співтовариства, але і виклик йому, про що недвозначно свідчать тривожні висловлювання лауреатів престижної серед програмістів премії імені Тьюринга[33].

Інформаційне суспільство – нова історична фаза розвитку цивілізації, у якій головними продуктами виробництва є дані й знання.

Створивши нове середовище – Інтернет, у якому комп'ютери – основний інструмент комунікації, людство змушене створити в ньому й норми поведінки. У цьому середовищі, кожен, хто занурюється в кібернетичний простір, зобов'язаний дбати не лише про себе, але й про оточуючих – про людей, із якими „спілкується", про інформаційні ресурси, із яких отримує дані чи інформацію або ж робить доступними власні. Тому, користуючись будь-якою свободою, слід пам'ятати, що вона обмежується свободою інших людей.

На думку Дж. Мура (розділ 1, п. 1.4), інформаційні технології в силу їх гнучкості можуть бути використані скрізь, причому несподіваним чином. Однак при цьому відчувається брак ціннісних установок і концептуальних прозрінь. Розмірковуючи над проектом комп'ютерної етики, він вирішив поставити на чільне місце наступні основні цінності: життя, здоров'я, щастя, безпека, природні багатства, сприятливі можливості і знання. Керуючись ними, необхідно забезпечити інтегральну цінність – справедливість.

Комп'ютерна революція породжує велику кількість проблем гуманітарного характеру, в тому числі принципово нові етичні питання. Користувачів мережевого простору, зокрема інтернету, зваблюють нові спокуси, властиві будь-якому іншому людському співтовариству, часто з відтінком антисоціальної поведінки. Тому з кожним роком дедалі актуальнішими стають питання регулювання відносин, зростає розуміння того, що саморегуляція на основі етичних норм є одним із способів співіснування у віртуальному світі.

В інтернет-середовищі виникає проблема збереження та підтримки етичних норм, дієвість яких у суспільстві визначається ставленням до проблеми державних органів, рівнем самосвідомості кожного індивіда, мірою та способами суспільного впливу в разі їх порушення. У США, Австралії, Великобританії та інших європейських країнах створені інститути, що досліджують проблеми

[33] Премія Тюрінга (англ. Turing Award) – найпрестижніша премія в галузі інформатики, щорічно присуджується Асоціацією обчислювальної техніки за видатні досягнення у цій галузі. Премія спонсорується корпораціями Intel та Google і зараз супроводжується нагородою в 1 000 000 доларів США.[1] Премію названо на честь видатного англійського вченого Алана Тюрінга, математика, фахівця з криптографії, який отримав перші глибокі результати щодо теорії алгоритмів та обчислювальної складності задовго до появи перших комп'ютерів.

соціального впливу комп'ютерних технологій на особистість і суспільство, а також розробляють відповідні рекомендації, норми й методи їх упровадження в суспільну свідомість. Нині комп'ютерно-етична проблематика вийшла далеко за рамки питань про межі етично припустимого застосування комп'ютерів створивши новий напрямок досліджень застосування етичних норм в інформатиці.

Інформаційна етика пов’язана з моральними проблемами, що виникають у зв’язку з розвитком і застосуванням інформаційних технологій.

Телекомунікаційні та комп’ютерні технології, глобальність інтернету не тільки відкривають нові вражаючі можливості для створення та поширення інформації й знань, а й створюють певну небезпеку виникнення суперечностей між цінностями, культурною спадщиною різних держав і народів. Складається така ситуація, коли майже в усіх користувачів інтернету не викликає сумніву корисність та необхідність міжнародної комп'ютерної мережі для сучасної життєдіяльності людства та його розвитку, але водночас виявляються складні проблеми взаємовпливу та взаємовідносин між інформаційною технологією та культурними традиціями й нормами поведінки особистості.

Інформаційна етика є складовою комп’ютерної етики, яку багато науковців називають цифровою етикою, і має глобальний характер, оскільки всі науки зводяться до інформатики (створення, оброблення, передача, отримання, зберігання інформації у всіх сферах людської діяльності).

Комп’ютерна етика пов’язана з розглядом технічних, моральних, юридичних, соціальних, політичних і філософських питань. Проблеми, що аналізовані в ній, можна розділити на кілька груп.

1. Проблеми розробки моральних кодексів для комп’ютерних професіоналів і простих користувачів, чия робота пов’язана з використанням комп’ютерної техніки.

2. Проблеми захисту прав власності, авторських прав, права на особисте життя і свободу слова щодо сфери інформаційних технологій.

3. Група проблем, що виникають з появою комп’ютерних злочинів, визначенням їхнього статусу, тобто переважно правові проблеми.

Зазначені проблеми є лише частиною комп’ютерної етики.

На думку англійського ученого Л. Флориді [40], інформаційна етика припускає, що існує щось більш елементарне й фундаментальне, ніж життя та страждання. Йдеться про буття взагалі, яке розуміється як інформація.

Узагальнюючи теоретичні погляди Л. Флориді на інформаційну етику, дослідники формулюють її основне завдання – оцінити з моральної точки зору будь-яку інформацію про все, що існує або існуватиме в світі, починаючи від людей і їх соціальних відносин і до зірок, каменів, тварин, рослин. Іншими словами, йдеться про морально-етичні норми по відношенню до будь-якої інформації, а не тільки до інформації, яка зафіксована та функціонує на комп'ютерних носіях, як це розуміється в площині комп'ютерної етики.

Інформаційна етика розглядає формування етичних стандартів та норм поведінки при створенні, поширенні та використанні інформації під час використання інформаційних технологій.

Коли заходить мова про інформаційну культуру, в першу чергу слід пам'ятати про моральні, законодавчі права, а також про етичну межу, яку не варто переходити навіть під час спілкування через монітор. У ці моменти слід пам'ятати про дружелюбність, культуру мовлення, стриманість, коректність та об'єктивність.

Етичний обов'язок - це стандарт, який визначає моральні дії. Вичерпні набори етичних зобов'язань поширюються на багато професій, в тому числі і на інформаційну та кібербезпеку і в разі їх порушення можуть призвести до санкцій.

Етичні проблеми кібербезпеки виходять за рамки найбільш загальновизнаних (наприклад, конфіденційність).

В останні роки спостерігається постійне зростання кількості організацій, які включають зобов'язання з кібербезпеки в свої етичні кодекси. Для ілюстрації в консультативному висновку «конфіденційність і технології», виданому адвокатурою штату Каліфорнія, зазначено: «Обов'язки адвоката щодо конфіденційності та компетентності вимагають від адвоката вжиття відповідних заходів для забезпечення того, щоб використання ним технологій спільно з представництвом клієнта не піддало невиправданому ризику несанкціонованого розголошення конфіденційної інформації клієнта. Через мінливий характер технологій та відмінності у функціях безпеки, які доступні, адвокат повинен переконатися, що кроки є достатніми для кожної форми технології, яка використовується, і повинен продовжувати стежити за ефективністю таких кроків».

Наприклад, Кодекс медичної етики, прийнятий Американською медичною асоціацією, встановлює цінності, яким кожен лікар зобов'язується як член медичної професії.

Враховуючи важливість сучасних технологій, можна очікувати, що кількість організацій, які покладають на своїх членів етичні зобов'язання з кібербезпеки, буде продовжувати зростати.

Кібербезпека - це процес захисту комп'ютерних систем, мереж, пристроїв та програм, підключених до Інтернету, від будь-якого типу кібератак та відновлення після будь-якого типу кібератаки. Така практика використовується як фізичними, так і юридичними особами для захисту від несанкціонованого доступу до центрів обробки даних та інших комп'ютеризованих систем. Кібератаки зараз становлять більшу загрозу для даних, оскільки кіберзлочинці обходять традиційний захист даних, використовуючи нові методи проникнення в систему, засновані на використанні соціальної психології та штучного інтелекту.

Управління кібербезпекою потребує перевірки та оцінювання її стану або аудит. При слові «аудит» перше, що спадає на думку – фінансові аудитори, які перевіряють звітність та іншу документацію в компанії. Проте коли ми говоримо про аудит інформаційних технологій, інформаційної безпеки або кібербезпеки, багато хто жартує про консультантів, які розповідають одне й те саме, надають поради без практичної користі, розмиті рекомендації, які клієнт міг би написати сам.

Важливою частиною аудиту є аналіз процесів управління і забезпечення кібербезпеки в компанії. У сучасній компанії сфера дії кібербезпеки, як правило, розподілена між цілою низкою департаментів: інформаційних технологій, інформаційної безпеки, управління відповідністю, управління кадрами, службою безпеки, внутрішнім аудитом і ще рядом інших підрозділів, які безпосередньо та опосередковано впливають на рівень кіберзахищеності. Оцінка ефективності та зрілості процесів управління кібербезпекою і взаємодії всіх цих елементів – основа проактивної роботи і ефективного реагування в разі кіберінцидентів або під час кібератаки. Результатом етапу є карта розвитку існуючих і впровадження нових процесів, які повинні забезпечити необхідний рівень кіберзахищеності бізнесу.

Технічна складова аудиту кібербезпеки також ширше, ніж просто інвентаризація програмних та апаратних засобів безпеки з вибірковим переглядом налаштувань. Це, в тому числі, зовнішнє і внутрішнє сканування для визначення вразливостей (навіть за наявності відповідного процесу та інструментів в компанії), а також проведення тестування на проникнення ззовні

і зсередини компанії (пентестінг[34]). Така незалежна оцінка має ще більший ефект, якщо проводиться «хвилею». Спочатку проводиться тестування на проникнення «наосліп» (Blackbox), потім проводиться аудит засобів безпеки і налаштувань, а потім проводиться «біле» тестування на проникнення (Whitebox) з усіма конфігураціями і доступами в ручному режимі. Результати етапу будуть цікаві технічним підрозділам і фахівцям, які матимуть практичну користь з рекомендацій, складених консультантами і «білими» хакерами.

При проведенні дослідження стану кібербезпеки виникають етичні проблеми, які потребують вирішення.

Для забезпечення узгодженості етичного нагляду перелік етичних питань структурований відповідно до принципів Менло[35] [41], опублікованих у 2012 році, щоб забезпечити узгодженість етичного нагляду за дослідженнями кібербезпеки.

Доповідь пропонує чотири принципи, які можуть бути використані для оцінки досліджень: повага до людей, доброчинство, справедливість та повага до закону та суспільних інтересів.

Повага до людей передбачає:

- участь як суб'єкта дослідження є добровільною і випливає з інформованої згоди;
- ставитися до окремих осіб як до автономних, самостійних агентів і поважати їх право визначати власні інтереси;
- поважайте осіб, які ще не є об'єктами досліджень;
- особи зі зменшеними можливостями, які не здатні вирішувати для себе, мають право на захист.

Інформована згода [42] є однією з основ етики дослідження стану кібербезпеки. Інформована згода (Informed consent) у кібербезпеці - це процес, за яким користувач погоджується з виконанням певних дій або збору даних з його сторони з повним розумінням можливих наслідків та ризиків. Це означає, що користувач повинен бути повністю проінформований про те, які дані збираються, як вони будуть використовуватися, хто має доступ до цих даних та як вони будуть зберігатися. Крім того, користувач повинен мати можливість відмовитися від збору своїх персональних даних, якщо він цього бажає.

[34] Тест на проникнення або пентест є одним із основних методів, що використовуються для виявлення областей системи, вразливих до вторгнень і компрометації.

[35] Принципи Менло (Menlo Principles) - це набір принципів для створення ефективних і стійких до змін програмних систем. Ці принципи були розроблені в рамках досліджень і робіт над програмними проектами компанії Menlo Innovations, що базується в місті Анн-Арбор, штат Мічиган, США.

Інформована згода у кібербезпеці є важливим елементом захисту персональних даних та приватності користувачів в Інтернеті, а також допомагає підвищити рівень безпеки в Інтернеті в цілому.

Здатність і акт отримання інформованої згоди від тих, хто постраждав від досліджень, відповідає Нюрнберзькому кодексу[36] і лежить в основі Гельсінської декларації[37] та Бельмонтської доповіді[38] [43-45].

Автори також зазначають, що «інформована згода ніколи не зменшує ризик для користувачів, це лише звільняє дослідників від певної відповідальності за цей ризик і навіть може збільшити ризик для користувачів, видаляючи будь-які сліди правдоподібного заперечення»

При проведенні досліджень часто виявляються персональні дані, які потім потрібно обробляти належним чином. Існує велика кількість робіт щодо визначення, обсягу та цінності конфіденційності, яка безпосередньо стосується дослідницької етики [46]. Однак будь-яке детальне обговорення єдиного етичного пункту швидко вийде за рамки теми обговорення. Але, не зважаючи на такий обсяг дискусій, питання конфіденційності продовжують виникати в дослідженнях кібербезпеки і сьогодні.

Не тільки етична але і юридична чутливість до проблем конфіденційності помітно різноманітна: Європейський загальний регламент про захист даних накладає суворі обмеження та каральні заходи на будь-яку взаємодію з даними, що стосуються європейських громадян, тоді як дані фізичних осіб в Америці, Азії чи Африці набагато менше підлягають регулюванню. Це може призвести до «демпінгу даних», в якому дослідження проводяться в країнах з нижчими бар'єрами для використання персональних даних, а не до того, щоб перестрибнути через бюрократичні перешкоди в Європі. Результатом є те, що дані неєвропейських громадян піддаються більш високому ризику, ніж у європейців.

[36] Нюрнберзький кодекс – міжнародний документ, який регулює принципи проведення медичних дослідів над людьми. Кодекс був розроблений і прийнятий після Нюрнберзького процесу над лікарями в 1947.

[37] Гельсінська декларація (англ. Declaration of Helsinki), розроблена Всесвітньою медичною асоціацією, являє собою набір етичних принципів для медичного співтовариства, стосуються експериментів на людях. Перша її редакція була прийнята в червні 1964 року в Гельсінки, Фінляндія, після чого зазнала вісім переглядів, останній в 2000 році.

[38] Бельмонтська доповідь або Звіт Бельмонта (Белмонта) (англ. Belmont Report) – повна назва: «Звіт Бельмонта: етичні принципи та рекомендації щодо захисту людей у рамках досліджень», «Звіт Національної комісії із захисту людей у рамках біомедичних та поведінкових досліджень». Звіт Бельмонта опублікований 30 вересня 1978 року Міністерством охорони здоров'я, освіти та соціального забезпечення США. Звіт Бельмонта включає настанови щодо захисту особистості людини, що бере участь у проведенні медичних досліджень, та основні етичні принципи проведення досліджень на людях і є основою для багатьох національних і міжнародних законів.

Під час виявлення персональних даних (ідентифікаційних даних) може виявитись додаткова інформація, що стосується фізичної особи чи організації. Необхідно заздалегідь прийняти рішення щодо того, чи слід і як інформувати цю організацію, якщо це доречно. Наприклад, можуть з'явитися докази того, що член організації шукає роботу в іншому місці, або що чоловік /дружина працівника має роман з іншим працівником. За відсутності політики, написаної заздалегідь, такі відкриття стають етичними дилемами, якими вони не повинні бути. Сьогодні невідомо про жодне академічне дослідження, яке б розглядало необхідність мати політику щодо випадкових висновків, що виникають внаслідок досліджень кібербезпеки. Так само, як принципи Менло спиралися на висновки Доповіді Бельмонта, було б розумно почати цей процес, спираючись на досвід медичної професії у вирішенні випадкових результатів, що виникають внаслідок експертиз та клінічних випробувань

Застосування цих чотирьох принципів на практиці не завжди є прямим, і для цього може знадобитися складне балансування. Наприклад, можна вважати, що повага до людей може заохотити роз'яснення, тоді як благополуччя його перешкоджає (якщо розгляд підсумків може сам по собі спричинити шкоду). Немає автоматичного способу збалансувати ці конкуруючі принципи, але вони допомагають прояснити компроміси, дають змогу дослідникам пояснити свої міркування один одному та громадськості, їх врахування може внести етичні зміни при проведенні аудиту кібербезпеки.

При проведенні досліджень стану кібербезпеки виникає питання щодо того, чи слід використовувати вразливості в системі безпеки для встановлення коду в цих системах. У деяких випадках дослідник повинен діяти як зловмисна сторона, щоб повністю протестувати систему, і це буде включати в себе використання вразливостей. Існують подібні випадки, коли дослідник може захотіти зайнятися фішинговими тестами, діючи як шкідливий агент при виборі використовуваних методів, з метою визначення вразливостей. Проте фішинг[39] за своєю природою використовує обман, і не можна легко отримати попередню інформовану згоду суб'єктів дослідження, побоюючись компрометації дослідження [47]. У невеликих масштабах експерименти з обмеженою участю дослідження без попередньої інформованої згоди та/або використання обману, коли шкода мінімальна, зазвичай вважаються прийнятною практикою, як,

[39] Фішинг – це форма атаки з використанням соціальної інженерії, в ході якої зловмисник, маскуючись під надійний суб'єкт, виманює конфіденційну інформацію жертв.

наприклад, при проведенні деяких психологічних досліджень, в яких досліджуваний аспект відрізняється від того, який, на думку учасників, є еталоном. Однак шкоду передбачити складніше, а відсутність згоди буде більш проблематичною, коли експеримент виходить за рамки декількох піддослідних. Фішинг і використання вразливостей для тестування системи можуть завдати великої шкоди причетним особам, коли не було отримано інформованої згоди. Саме тому слід уникати всякої шкоди, якщо це взагалі можливо. Там, де уникнення неможливе, можуть бути корисними етичні комісії, допомагаючи визначити пропорційність шкоди дослідженню.

Якщо виявляються вразливості, чи повинні вони бути розкриті відповідному органу влади? Таким органом може бути компанія, яка використовує програмне забезпечення, що має вразливість, сторонній постачальник цього програмного забезпечення або державна організація, яка здійснює нагляд за вразливостями. В принципі, широке усвідомлення вразливостей є позитивним, оскільки може допомогти спільноті об'єднатися, щоб отримати чітке уявлення про те, наскільки широко поширена вразливість, чи були розроблені будь-які пропрієтарні патчі[40] та чи була використана вразливість. Однак існує також ризик трансляції вразливості навіть у невеликій спільноті фахівців з кібербезпеки, імовірність що знання про цю вразливість просочиться і таким чином може бути використане. Однак, не зважаючи на знання про цінність і необхідність розкриття вразливостей, у світі відомо лише про кілька університетських комісії з етики проведення досліджень, які мають політику щодо розкриття вразливостей.

Можливо, навіть вразливості будуть виявлені в ході досліджень кібербезпеки, і дуже важливо, щоб ті, хто наглядає за цим дослідженням, мали чіткі вказівки щодо того, що має статися за таких обставин. Додатковою перевагою політики розкриття вразливостей буде захист дослідника у випадках, коли вразливості виявлені, але інформована згода не була отримана. У таких випадках існує високий ризик того, що постраждала сторона притягне до відповідальності університет або дослідника. У таких випадках чи є ще обов'язок зробити ці відкриття відомими? Який ступінь ризику повинен обтяжувати дослідник і науково-дослідна установа при дослідженні таких вразливостей?

[40] Пропрієтарне програмне забезпечення , (від англ. proprietary software) – це програмне забезпечення, на яке зберігаються як немайнові, так і майнові авторські права . Отримавши або придбавши таке програмне забезпечення, користувач отримує обмежені права користування ним: може бути заборонено або закрито доступ до коду (вивчення), внесення змін, тиражування, розповсюдження та перепродажа.. .

Відповіді на них будуть відрізнятися залежно від установи, але ясність знову ж таки необхідна для захисту дослідника.

Нижче ми розглянемо три основні проблеми, пов'язані з етичними зобов'язаннями з кібербезпеки, а саме: невизначеність, викликана широкими зобов'язаннями, легкий обхід, труднощі, пов'язані з контролем дотримання вимог.

Невизначеність, викликана широкими зобов'язаннями.

Положення, що містять етичні зобов'язання з кібербезпеки, часто включають широкі терміни, такі як "відповідні кроки", "достатні заходи", "розумні зусилля" та "невиправданий ризик". Оскільки такі терміни настільки широкі, вони близькі до безглуздих. Наприклад, вищезгаданий консультативний висновок колегії адвокатів, який вимагає від кожного адвоката в Каліфорнії вжити відповідних заходів для забезпечення того, щоб використання технологій не піддало конфіденційну інформацію клієнта невиправданому ризику. Незрозуміло, чи включають відповідні заходи такі кроки, як надійні паролі, сучасне антивірусне програмне забезпечення, регулярне навчання з інформаційної безпеки та політику реагування на інциденти. Крім того, якщо людина здійснить велику кількість кроків, але не здійснить один важливий крок, вона все одно може вважатися такою, що вжила «відповідних кроків». Це пояснюється тим, що термін «відповідні кроки» не означає «всі можливі кроки». У сфері інформаційної безпеки достатньо однієї слабкості інформаційної безпеки (наприклад, використання слабкого пароля), щоб дозволити злочинцю скомпрометувати цілу мережу.

Легкий обхід.

Етичні зобов'язання з кібербезпеки часто легко обійти. Наприклад, Правила професійної поведінки юристів Нью-Йорка вимагають від них тримати руку на пульсі переваг і ризиків, пов'язаних з технологіями, які адвокат використовує для надання послуг клієнтам або для зберігання, або для передачі конфіденційної інформації. Довести дотримання цього обов'язку можна легко, підписавшись на кілька журналів з інформаційної безпеки і регулярно відвідуючи курси в сфері інформаційної безпеки. Однак ні журнали, ні курси не гарантують, що людина тримає руку на пульсі переваг і ризиків, пов'язаних з технологіями. Єдиний спосіб перевірити дотримання такого етичного обов'язку - вимагати від юристів проходження тестів на інформаційну безпеку.

Труднощі, пов'язані з контролем відповідності.

Багато організацій не прийняли процедури точної оцінки відповідності своїх членів застосовним етичним зобов'язанням з кібербезпеки. Приймаючи такі процедури та публікуючи вичерпну інформацію про них, організації сприятимуть дотриманню попередньої оцінки етичних зобов'язань щодо кібербезпеки. Процедури можуть, наприклад, включати детальний перелік критеріїв, що використовуються для оцінки відповідності, анкетування та інтерв'ю.

Вирішення проблем, пов'язаних з етичними зобов'язаннями щодо кібербезпеки.

Три проблеми, згадані в попередньому розділі, можна вирішити, прийнявши конкретні зобов'язання, додавши механізми боротьби з обходом і встановивши процедури контролю за дотриманням вимог.

Прийняття конкретних зобов'язань.

Організації можуть вказати свої зобов'язання щодо кібербезпеки, перерахувавши мінімальні заходи, які слід вжити для забезпечення відповідності. Такі заходи можуть включати угоди про конфіденційність, порядок і механізми сканування вразливостей, навчання з питань безпеки, безпечну утилізацію обладнання, планування аварійного відновлення, резервне копіювання інформації, класифікацію даних, безпеку паролів, блокування неактивних обчислювальних пристроїв, захист мережевої інфраструктури, планування реагування на інциденти та звітування про інциденти. Кожне з конкретних зобов'язань, включених в етичний кодекс організації, має бути ретельно опрацьовано.

Хороший приклад конкретних зобов'язань з кібербезпеки можна знайти в законі штату Массачусетс (M.G.L. c. 93H), який вимагає від осіб, які збирають певну особисту інформацію, застосовувати заходи інформаційної безпеки, включаючи: «Шифрування всіх переданих записів і файлів, що містять особисту інформацію, яка буде переміщатися по загальнодоступних мережах, і шифрування всіх даних, що містять особисту інформацію, що підлягають передачі по бездротовому зв'язку. Шифрування всієї особистої інформації, що зберігається на ноутбуках або інших портативних пристроях.»

Вимагаючи від осіб, які збирають персональні дані, використовувати шифрування, закон гарантує, що зібрані ними персональні дані будуть захищені від несанкціонованого доступу.

Інші заходи, які підходять для захисту персональних даних, включають приховування інформації та захищене паролем стиснення без втрат. Приховування інформації відноситься до процесу приховування інформації, наприклад, шляхом поділу інформації на частини, які повинні бути зібрані для використання інформації. Стиснення без втрат – це тип стиснення даних, який дозволяє повністю реконструювати вихідні дані зі стиснутих даних. Оскільки стиснення з втратами зменшує файли, постійно усуваючи інформацію, це може призвести до втрати важливої особистої інформації. Стиснення з втратами може бути придатним для стиснення особистої інформації лише в тому випадку, якщо інформація має форму відео або зображень і спотворення стиснених відео або зображень непомітні.

Додавання механізмів проти обходу.

Найкращим способом уникнути обходу етичних зобов'язань є нав'язування механізмів обходу, таких як аудит інформаційної безпеки незалежними експертами. Такі аудити дозволять організаціям з'ясувати, чи дотримуються їхні члени застосовних зобов'язань щодо кібербезпеки, чи вони просто забезпечують «відповідність паперу» (наприклад, мають політику безпеки, але не реалізують її на практиці). Аудит інформаційної безпеки може приймати дві форми, а саме ручні аудити та автоматичні аудити.

Ручні аудити можуть включати сканування вразливостей безпеки, огляди засобів контролю доступу та проведення інтерв'ю з працівниками.

Автоматизовані аудити можуть включати в себе звіти, сформовані програмним забезпеченням, автоматичний моніторинг комп'ютерних систем і автоматичне звітування про інциденти.

Незалежно від його виду, кожен аудит повинен ґрунтуватися на керівних принципах аудиту, які вказують на цілі, методології та результати аудиту, а також інструменти, що використовуються для проведення аудиту. Якщо аудит виконується вручну, методичні рекомендації повинні бути у вигляді технічного завдання, заздалегідь наданого аудитором. Інструменти, що використовуються для проведення аудиту, можуть варіюватися від простих контрольних списків завдань, які повинні бути виконані в ході аудиту, до передових інструментів оцінки вразливостей, призначених для виявлення недоліків в комп'ютерних системах.

Встановлення процедур контролю за дотриманням вимог.

Процедури моніторингу відповідності не повинні контролювати всі кінцеві точки, мережі, програми, інфраструктуру, системи та процеси. Досить, якщо процедури будуть моніторити сегменти помірного і високого впливу. Наприклад, загальнодоступний веб-сервер, який містить загальнодоступну інформацію та не збирає персональні дані, може розглядатися як сегмент низького впливу. У свою чергу, базу даних, що містить конфіденційні персональні дані (наприклад, дані про стан здоров'я, дані кредитної картки, сексуальну орієнтацію, біометричні дані, політичну та релігійну приналежність), слід розглядати як сегмент високого впливу. Слід зазначити, що контрольовані сегменти також повинні покривати хмару. Хмарний моніторинг може бути складною проблемою, оскільки інформація, що зберігається в хмарі, зазвичай фрагментована та розосереджена у великій кількості країн.

Після прийняття рішення про те, які сегменти моніторити, необхідно визначити інтервали моніторингу. Безперервний моніторинг і звітність можуть бути обтяжливими і вимагати значних ресурсів. Національний інститут стандартів і технологій рекомендує наступні інтервали моніторингу аналізу зібраних даних журналів:

- сегменти з низьким рівнем впливу – не рідше одного разу на 1-7 днів;
- системи з помірним впливом – принаймні раз на 12-24 години;
- системи з високим рівнем впливу – не менше шести разів на день.

Результати аудитів відповідності, як правило, можна розділити на три категорії, а саме:

- відповідність;
- необхідна подальша оцінка;
- відсутність відповідності.

Перша категорія вказує на те, що перевірені системи відповідають застосовним етичним зобов'язанням з кібербезпеки. Друга категорія вказує на те, що зібраний зворотний зв'язок потребує подальшого вивчення і, можливо, буде потрібно провести додаткову оцінку перевірених систем. Третя категорія сигналізує про те, що перевірені системи не відповідають вимогам.

Висновки. Все більше організацій включають зобов'язання з кібербезпеки в свої етичні кодекси. Порушення цих зобов'язань може призвести до фінансових, дисциплінарних та репутаційних наслідків. Щоб захистити своїх членів від необґрунтованих санкцій та забезпечити ефективне дотримання

етичних зобов'язань щодо кібербезпеки, організації повинні використовувати конкретні зобов'язання щодо кібербезпеки, використовувати механізми боротьби з обходом та встановлювати процедури моніторингу відповідності.

Особи, які бажають пом'якшити наслідки ненавмисного недотримання етичних зобов'язань щодо кібербезпеки, можуть придбати кіберстрахування. Він покриє не тільки збитки, спричинені інцидентами кібербезпеки, але й витрати, понесені у зв'язку з розслідуванням та реагуванням на них. Деякі поліси кіберстрахування можуть навіть покривати виплату викупу, який потрібно заплатити за розшифровку файлів, зашифрованих програмами-вимагачами, такими як CTB-Locker і TeslaCrypt.

 *Питання для самоконтролю*:

1.На чому ґрунтується інформаційна культура?

2.Чому інформаційну та комп’ютерну етику ототожнюють з цифровою?

3.Як принципи Нюрнберзького кодексу стосуються кібербезпеки?

 *Завдання:*

1. Зробити аналіз отримання премії Тьюрінга за роки її існування: хто, за що, з якої країни, який внесок у кібербезпеку?
2. Описати інформаційні процеси, які відбуваються під час вашої навчальної діяльності. Наведіть приклади технологій і засобів реалізації цих процесів.
3. У вправі за посиланням http://LeamingApps.org/watch?v=p502ii7et16 відтворити текст про дотримання правил інформаційної етики та закону про авторське право.

2.3. Етика хакера

Культура хакерів та відповідна філософія зародилися в Массачусетському технологічному інституті (MTI) в 1950-тих та 60-тих. Термін хакерська етика вперше був використаний журналістом Стівеном Леві у його книжці 1984-го року «Хакери: Герої комп'ютерної революції». Хоча деякі принципи етики хакерів були описані в інших текстах на зразок «Computer Lib/Dream Machines»

(1974) Теда Нельсона. Леві вважається першим, хто задокументував як саму філософію, так і її засновників.

Леві пояснює, що MTI утримував один з перших комп'ютерів IBM 704 у 1959 всередині кімнати Electronic Accounting Machinery (EAM). Ця кімната стала місцем появи хакерів, коли студенти MTI з клубу технічного моделювання залізниці пробирались сюди після годинних спроб запрограмувати 30-тонний комп'ютер триметрової висоти.

Під словом «хак» (англ. hack) мали на увазі проект чи продукт, створений не лише з певною конструктивною ціллю, але і для того, щоб відчути задоволення від процесу участі у творенні.[48-50]. Термін хак був запозичений зі сленгу MTI, де це слово означало жартівливі витівки, що регулярно здійснювались студентами. Щоправда, сьогодні етику хакерів часто цитують поза контекстом та помилково прив'язують її до хаку як діяльності щодо зламу та проникнення в комп'ютерні системи, а багато джерел помилково вважають, що ця етика стосується білих капелюхів. Але те, про що писав Леві, стосується не так комп'ютерної безпеки, як ширших питань.

Хакерська етика описується як «новий спосіб життя, з філософією, етикою та мрією». Елементи хакерської етики не були відкрито обговорюваними, вони скоріше були неявно прийняті з мовчазною згодою [49] .

Рух за вільне програмне забезпечення народився на початку 80-тих з послідовників хакерської етики. Його засновник, Річард Столмен, описується Стівеном Леві як «останній справжній хакер».[48] Сучасні хакери, які залишаються вірними своїй етиці, особливо практичному імперативу, зазвичай є прихильниками вільного та відкритого ПЗ. Це пов'язано з тим, що вільне та відкрите програмне забезпечення дозволяє хакерам отримувати доступ до коду, використаного для створення програмного забезпечення, та вдосконалювати його чи використовувати в своїх проектах.

Річард Столлмен[41] описував суть хакерської етики таким чином: «Хакерська етика стосується відчуття того, що добре, а що погано, етичних ідей, що має ця спільнота людей – що знання повинні поширюватись серед інших людей, які можуть отримати від них користь, і що важливі ресурси повинні використовуватися, а не витрачатись

[41] Ри́чард Ме́тью Сто́лмен (англ. Richard Stallman; часто rms (за ініціалами); нар. 16 березня 1953, Нью-Йорк) – засновник руху вільного ПЗ, проєкту GNU, Фонду вільних програм та Ліги за свободу програмування.

марно.». Він уточнював, що хакінг, який означався ним як грайлива здібність, та етика є двома різними поняттями: «Те, що комусь просто подобається хакінг, ще не означає, що він має етичне зобов'язання відповідно ставитись до інших. Деякі хакери турбуються про етику, як, наприклад, я, але це не є обов'язковою ознакою хакера, це окрема якість. Хакінг не стосується перш за все етичних питань. … хакінг часто приводить значне число хакерів до роздумів над певними етичними питаннями з певних сторін. Я не хочу цілком заперечувати всі зв'язки між хакінгом та поглядами на етику.»

Як Леві підсумував в передмові до «Хакерів», загальні догми чи принципи хакерської етики включають [48] :

- необхідність ділитися з іншими;
- відкритість;
- децентралізація;
- вільний доступ до комп'ютерів;
- вдосконалення світу.

На додачу до цих принципів Леві також описав хакерську етику та їх погляди: «Доступ до комп'ютерів та всього, що містить дані про те, як працює світ, повинен бути необмеженим та загальним. Завжди підкоряйтесь Практичному Імперативу!».

Леві перелічує здібності хакерів до навчання та створення чогось на основі наявних ідей та систем. Він вірить, що вільний доступ до програм дає хакерам можливість розбирати речі на частини, ремонтувати чи вдосконалювати їх та вивчати й розуміти принципи їх роботи. Це дає їм знання для створення нових та навіть цікавіших речей. Доступ допомагає поширенню технології.

Вся інформація повинна бути вільною.

Виходячи прямо з принципу доступу, можна сказати, що інформація повинна бути вільнодоступною для отримання, виправлення, вдосконалення та перевинайдення. Вільний обмін інформацією загалом стимулює творчість. З точки зору хакера, будь-яка система може виграти від вільного потоку інформації. Ця ідея у соціальних науках відома як прозорість. Як зауважує Річард Столмен, «вільний» стосується необмеженого доступу, а не ціни.

Один із принципів етичних хакерів – «Не довіряй авторитету – пропагуй децентралізацію». Найкращий спосіб пропагувати вільний обмін інформацією – мати відкриту систему, яка не створює кордонів між хакером та інформацією чи елементом обладнання, які потрібні йому на його шляху до знань та

вдосконалення. Хакери вірять, що бюрократії, корпоративні, урядові чи університетські, є недосконалими системами.

Хакера потрібно оцінювати за результатами його діяльності, а не за званням, віком, расою, статтю чи посадою.

Хакерська етика є меритократичною системою[42], де рангами нехтують на користь навичок. Леві виразно показує, що такі критерії як вік, стать, раса, посада та дипломи вважались недоречними в спільноті хакерів. Навички хакера є остаточним визначником прийняття. Такий кодекс всередині хакерської спільноти сприяє поширенню розвитку хакінгу та розробки програмного забезпечення. Як приклад етики рівних можливостей, наводиться Пітер Дойч, дванадцятилітній хакер, якого прийняли в спільноту TX-0[43], хоча його не визнавали аспіранти не-хакери.

За допомогою комп'ютера можна творити красу й мистецтво.

Хакери глибоко цінували інноваційні технології, які дозволяли програмам виконувати складні задачі за допомогою кількох інструкцій. Вважалося, що код програми гарний сам по собі, якщо він був дбайливо написаний та мистецьки організований. Створення програм, що займали найменший об'єм місця, майже стало змаганням серед перших хакерів.

Комп'ютери можуть покращити життя.

Хакери відчували, що комп'ютери збагатили їх життя, дали їхньому життю фокус та наповнили його пригодами. Хакери розглядали комп'ютери як Лампи Алладіна, які вони можуть контролювати. Вони вірили, що будь-хто в суспільстві може виграти від такого досвіду і, якщо кожен зможе взаємодіяти з комп'ютерами у такий спосіб, як це робили хакери, то хакерська етика поширюється суспільством і комп'ютери вдосконалять світ.

Багато принципів та догм етики хакерів направлені до спільної мети: Практичного Імперативу[44]. Як Леві описує, «Хакери вірять, що суттєві знання про системи й про світ можна отримати, розбираючи речі на частини, спостерігаючи за їх роботою та використовуючи ці знання, щоб створювати більш нові та цікаві речі.» [48].

---

[42] Меритократичність – це питомість системи організації праці, при котрій панує орієнтація на заохочення здобутків й ефективності («кожному – за здатностями»).

[43] TX-0 (скор. від англ. Transistorized Experimental computer zero), також згадуваний як tixo (вимовляється «тіксо») – один з перших комп'ютерів створених повністю на транзисторній базі та, та що мав для свого часу величезний обсяг пам'яті на магнітних сердечниках в 64K 18-бітних слів. TX-0 був введений в експлуатацію в 1956-му і безперервно використовувався до 1960-х років

[44] Практичний імператив, сформований І. Кантом: «Вчиняй так, щоб ти завжди, і в особі своїй, і в особі іншого, ставився до людей як до мети, цілі, а ніколи не відносився до них тільки як до засобу.»

Застосування Практичного Імперативу вимагає вільного доступу, відкритої інформації та поширення знань. Мета справжнього хакера – обійти обмеження Практичного Імперативу – виправдовує засоби. Коли ці принципи відсутні, хакери намагаються їх обійти. Наприклад, коли комп'ютери в MTI захищались фізичними замками чи програмами логіну, хакери систематично їх обходили, щоб мати доступ до машин. Хакери допускали «навмисну сліпоту» в погоні за досконалістю. Ця поведінка не була шкідливою за природою: хакери MTI не намагались завдати шкоди системам чи їх користувачам (хоча випадкові жарти іноді здійснювались з допомогою комп'ютерних систем). Це глибоко контрастує з сучасним, уявленням хакера, спровокованим мас-медіа, який зламує комп'ютерні системи, щоб вкрасти інформацію чи здійснити кібер-вандалізм.

Леві ідентифікував кількох «справжніх хакерів», які значно вплинули на хакерську етику. Деякими з добре відомих «справжніх хакерів» є:

– Джон Маккарті, співзасновник Лабораторії штучного інтелекту MTI та Стенфорської лабораторії штучного інтелекту;
– Біл Госпер, математик та хакер;
– Річард Грінблатт, програміст та ранній розробник LISP машин;
– Річард Столммен, програміст та громадський діяч, який добре відомий завдяки GNU[45], Emacs[46] та руху за вільне програмне забезпечення.

Леві також ідентифікує «хакерів заліза» («друге покоління» з центром переважно в Кремнієвій долині) та «хакерів ігор» («третє покоління»). Всі три покоління хакерів, згідно з Леві, втілювали принципи хакерської етики. Деякими з хакерів «другого покоління» були:

- Стів Возняк, один з засновників Apple Computer;
- Боб Марш, розробник комп'ютера Sol-20;
- Фред Мур, громадський діяч та засновник Homebrew Computer Club;
- Стів Домпіер, член Homebrew Computer Club та хакер, який працював з Altair 8800;
- Лі Фелсенштейн, хакер заліза та співзасновник проекту Community Memory та Homebrew Computer Club, розробник комп'ютера Sol-20;
- Джон Драпер, легендарна особистість в світі програмування, він написав EasyWriter, перший текстовий процесор.

[45] GNU (/gnu:/ (слухати)) - це велика колекція вільного програмного забезпечення (383 пакети станом на січень 2022 року), які можуть використовуватися як операційна система або можуть використовуватися по частинах з іншими операційними системами.

[46] Emacs /ˈiːmæks/, спочатку названий EMACS (абревіатура від «Редактор MACroS») - це сімейство текстових редакторів, які характеризуються своєю розширюваністю.

До діячів «третього покоління» Леві відніс:

- Джона Харріса, одного з перших програмістів, найнятих компанією On-Line Systems (яка пізніше стала Sierra Entertainment);
- Кена Вільямса разом з дружиною Робертою, який заснував On-Line Systems після роботи в IBM.

Стівен Мізрач, який ідентифікує себе як дослідника кіберантропології, порівняв «Стару етику хакерів» Леві, з «Новою етикою хакерів», яка переважає в спільноті спеціалістів з комп'ютерної безпеки. В своєму есе, названому «Чи є етика для хакерів 90-тих?» він робить контроверсійне твердження, що «Нова етика хакерів» поступово розвинулась із старої, хоча й пережила радикальний зсув. Але, не зважаючи на те, що природа хакерської діяльності змінилась через доступність нових технологій (наприклад, поширення персональних комп'ютерів чи соціальну пов'язаність інтернету), аспекти етики хакерів, особливо ті, що стосуються доступу, спільного використання та спільноти, – залишились незмінними.

В 2001-му фінський філософ Пекка Хіманен [51] пропагував хакерську етику на противагу Протестантській етиці праці[47]. На думку Хіманена, етика хакерів більш тісно пов'язана з етикою чеснот, яку знаходимо в записах Платона та Аристотеля. Автор пише про етику хакерів, яка обертається навколо пристрасті, важкої праці, творчості та задоволення від створення програмного забезпечення.

Різниця між хакером і кракером.

В основному думка комп'ютерного світу про хакерів або суто негативна (хакери – це злочинці), або скромно позитивна (хакери – санітари лісу). Насправді у цієї проблеми існує щонайменше дві сторони: одна позитивна, інша – негативна і між ними проходить чітка межа. Ця межа розділяє всіх професіоналів, пов'язаних з інформаційною безпекою, на хакерів (hackers) і кракерів (crackers).

І ті і інші займаються в переважній більшості рішенням одних і тих же задач – пошуком недоліків в обчислювальних системах і здійсненням атак на дані системи – але найголовніша і принципова відмінність між хакерами і кракерами полягає в цілях, які вони переслідують.

[47] Протестантська трудова етика (англ. Protestant work ethic; нім. Protestantische Arbeitsethik), також, кальвіністська трудова етика (нід. Calvinistische arbeidsethos; англ. Calvinist work ethic), або пуританська трудова етика (англ. Puritan work ethic) – доктрина в соціології, економіці та політології, заснована на релігійних біблійних цінностях, що представляють систему принципів чесності, праці та мотивації до розвитку

Основна задача хакера, досліджуючи обчислювальну систему, знайти слабкі місця в її системі безпеки з метою інформування користувачів і розробників системи для подальшого усунення знайдених недоліків.

Інша задача хакера, проаналізувавши існуючі недоліки захисту обчислювальної системи, сформулювати необхідні вимоги і умови підвищення рівня її захищеності.

Основна задача *кракера* полягає в безпосередньому здійсненні злому системи з метою отримання несанкціонованого доступу до чужої інформації – інакше кажучи, для її крадіжки, підміни або для оголошення факту злому.

Тобто, кракер, за своєю суттю, нічим не відрізняється від звичайного злодія, що зламує чужі квартири і краде чужі речі. Кракер зламує чужі обчислювальні системи і краде чужу інформацію. Ось в чому полягає кардинальна відмінність між тими, кого можна назвати хакерами і кракерами: перші – дослідники комп'ютерної безпеки, другі – просто зломщики, злодії або вандали.

Кракерів поділяють на категорії [52]:

1. *Вандали*: найвідоміша (багато в чому завдяки повсякденності вірусів) і, треба сказати, найменш численна частина кракерів. Їх основна мета – зламати систему для її руйнування. До них можна віднести, фахівців в написанні вірусів або троянських коней. Абсолютно природно, що весь комп'ютерний світ ненавидить кракерів–вандалів лютою ненавистю. Ця стадія кракерства звичайно характерна для новачків і швидко проходить, якщо кракеру вдається удосконалюватися (адже досить нудно усвідомлювати свою перевагу над беззахисними користувачами).

2. *Жартівники*: найменш шкідлива частина кракерів, основна мета яких – популярність, що досягається шляхом злому комп'ютерних систем і внесенням туди різних ефектів, що виражають їх незадоволене відчуття гумору. «Жартівники» – звичайно не завдають істотного збитку (хіба що морального). На сьогоднішній день в Internet це найпоширеніший клас кракерів, здійснюючих злом Web–серверів, залишаючи там згадку про себе. До жартівників також можна віднести творців вірусів, з різними візуально-звуковими ефектами (музика, тремтіння або перевертання екрану, малювання всіляких картинок і т. д.). Все це, в принципі, або безневинні витівки початківців, або – рекламні акції професіоналів.

3. *Взломщики*: професійні кракери, що користуються найбільшою пошаною в кракерському середовищі, основна задача яких – злом комп'ютерної системи з серйозною метою, будь то крадіжка або підміна інформації, що зберігається там. У загальному випадку, для того, щоб здійснити злом системи, необхідно пройти три основні стадії: дослідження обчислювальної системи з виявленням в ній недоліків, розробка програмної реалізації атаки і безпосереднє її здійснення. Справжнім професіоналом вважають того кракера, який для досягнення своє цілі проходить всі три стадії.

4. *Фрікери* (українською мовою "частотники") – це особи, які займаються розшифруванням супутникових сигналів з метою безкоштовного перегляду платних (кодованих) телевізійних каналів, "переадресуванням" мобільних телефонів з метою їх безоплатного використання. Здійснюється це шляхом перепрограмування ПЗУ мобільних телефонів, зломом АТС для безоплатного використання міжнародного зв'язку і т. ін. В Україні фрікерські групи поки що не відомі. Але такі особи часто входять в різні хакерські організації, а за кордоном деякі з них є президентами "фрікерських підгруп".

5. *Кардери*, які розкрадають кошти з чужих кредитних карток. Кардер встановлює номер того чи іншого власника кредитної картки, може замовити по цих картках товари по телефону або через комп'ютерну мережу. До них можна віднести також виготовлення чи підроблення фальшивих кредитних карток, за допомогою яких також розкрадаються кошти.

Більшість крекерів мають клички – прізвиська, за якими вони відомі серед інших крекерів. Вибір кличок, як правило, пов'язаний з віком та інтересами хакерів і крекерів. Ось деякі найбільш поширені з них: Скорпіон (Scorpion), Бандит (Bandito), Капітан (Captain), Розбещенець (Corrupt), Король Таран (Taran King), Скажений Едік (Crazy Eddic), Рейнджер Рік (Ranger Rick), Мисливець за головами (Head Hunter), Червоний лицар (Red Knight), Шпигун (Spy), Оратор (Orator) та багато інших [50]. Більшість з них свідчить про моральні якості їх власників, зокрема вони підкреслюють виклик і культ грубої сили. При спілкуванні хакери також широко використовують свій власний мовний жаргон.

Висновок. Отже, хакери є унікальною спільнотою людей, які мають свій світогляд, етику поведінки, стиль життя, атрибути та кумирів. Справжні хакери створюють речі, а не руйнують їх. Хакер повинен отримувати насолоду від вирішення проблем, тренування інтелекту. Він постійно прагне вирішувати нові, складні проблеми, а не перейматися монотонною діяльністю. Саме ці риси

відрізняють хакерів від сірої маси та інших субкультур, що доводить їхню унікальність.

 *Питання для самоконтролю*:

1.Що означає слово «хак»?

2.На скільки етичні принципи хакерів у сфері кібербезпеки?

3.В чому відмінність хакерів і кракерів?

 *Завдання:*

1.Знайти в мережі Інтернет інформацію про відомих хакерів та кракерів і їх досягнення.

2.4. Етичні проблеми створення і застосування штучного інтелекту в кібербезпеці

Застосування штучного інтелекту – процес активного використання найсучасніших наукових досягнень у сфері інформатики в різноманітних галузях життєдіяльності суспільства.

На теперішній час термін – «Штучний інтелект» (ШІ) вже надійно укорінився у повсякденному житті. І хоча пристроям з елементами штучного інтелекту все ще бракує можливостей зрозуміти проблему та знайти її рішення, то, коли йдеться про зменшення помилок в оперативних завданнях та пошук аномалій у різноманітних процесах, штучний інтелект випереджає людські здібності та компетентність. Штучний інтелект відіграє важливу роль у оцінці помилок, які можуть бути вчинені людьми. Передбачається, що у сфері кібербезпеки системи на основі штучного інтелекту зможуть захистити організації від Інтернет-загроз, визначати типи шкідливих програм, забезпечувати дотримування стандартів безпеки та допоможуть створити кращі стратегії запобігання атакам та відновлення після атак [53].

За оцінкою Gartner[48], витрати на системи інформаційної безпеки і управління ризиками у 2022-му році збільшились до $ 174 млрд, з них приблизно $ 50 млрд будуть спрямовані на захист клієнтських систем. Продажі хмарних платформ і додатків для забезпечення безпеки виростуть до $ 1,63 млрд в 2023-му році, а систем забезпечення безпеки додатків до $ 4,5 млрд.

Зростає і ринок послуг в області інформаційної безпеки, за останній рік він збільшився з $ 62 млрд до $ 66,9 млрд. Однак самі по собі гроші не можуть вирішити питання. Більшість фахівців з інформаційної безпеки сьогодні перевантажені аналізом журналів, запобіганням спроб злому, розслідуванням можливих випадків шахрайства і т. д. Дефіцит кадрів великий, тому в індустрії безпеки все з більшою надією дивляться на рішення в області штучного інтелекту. За оцінкою Marketsand Markets, в 2019-2026 рр. зростання ринку засобів ШІ для забезпечення кібербезпеки буде рости в середньому на 23,3% в рік, з $ 8,8 млрд до $ 38,2 млрд.

Штучний інтелект має стати інструментом, який допоможе спеціалістам з кібербезпеки виявляти зловмисників. Проте дослідження Wakefield Research[49], підготовлене на замовлення компанії Devo, говорить про те, що багато над чим треба працювати.

Штучний інтелект є предметом захоплення протягом десятиліть. Андроїди, вигадані письменником-фантастом Філіпом К. Діком, залишаються наразі науковою фантастикою, натомість штучний інтелект є цілком реальним і відіграє все більшу роль у багатьох аспектах нашого життя.

Звісно, цікаво спостерігати за дискусією щодо за і проти людиноподібних роботів із ШІ, проте тема використання ШІ в кібербезпеці не менш цікава і починає набирати все більше обертів.

Суть полягає в тому, щоб штучний інтелект підсилював команди професіоналів з безпеки. Як показує дослідження, аналітики SOC (Security Operations Center, Центр Інформаційної Безпеки) часто перевантажені нескінченною кількістю попереджень, які щодня з’являються на їхніх екранах. Втома від тривоги стала причиною вигорання аналітиків для всієї галузі.

[48] Gartner, Inc. - це технологічна дослідницька та консалтингова фірма, що базується в Стемфорді, штат Коннектикут, яка проводить дослідження технологій та ділиться цим дослідженням як за допомогою приватного консалтингу, так і через виконавчі програми та конференції.

[49] Wakefield Research, компанія з дослідження ринку, співпрацює з найбільшими брендами та агентствами світу майже в 100 країнах.

В ідеалі штучний інтелект міг би допомогти аналітикам SOC йти в ногу та випереджати розумних і спритних хакерів, які ефективно використовують ШІ для злочинних чи шпигунських дій. Але, на жаль, поки що цього не відбувається.

ІЛЛЮЗІЯ Штучного Інтелекту.

В рамках дослідження SOC [54] було проведено опитування 200 фахівців з ІТ-безпеки, щоб визначити, як вони ставляться до ШІ. Опитування покриває тему впровадження штучного інтелекту, що охоплює низку елементів захисту, включаючи виявлення загроз, прогнозування ризику зламу та реагування/управління інцидентами.

Міф №1: кібербезпека на основі ШІ вже існує.

Усі респонденти сказали, що їхня організація використовує ШІ в одній або кількох сферах. Найпопулярнішою сферою використання є управління інвентаризацією ІТ-активів, потім виявлення загроз (що є гарною новиною) і прогнозування ризиків зламу.

Але з точки зору використання штучного інтелекту безпосередньо в боротьбі із зловмисниками, на даний момент про це не йдеться. Приблизно 67% респондентів сказали, що їхня організація використовує штучний інтелект «дуже й дуже поверхнево».

В якій мірі організації розраховують на штучний інтелект у кібербезпеці?

Більше половини респондентів вважають, що їхня організація – принаймні зараз – надто покладається на ШІ. Менше однієї третини вважають, що є доцільним покладатися на штучний інтелект, тоді як меншість респондентів вважає, що їхня організація недостатньо використовує штучний інтелект.

Міф №2: ШІ вирішить проблеми безпеки.

Коли респондентів запитали їхню думку щодо проблем, пов’язаних із використанням штучного інтелекту в їхніх організаціях, вони не соромилися. Лише 7% респондентів сказали, що не стикалися з проблемами використання ШІ у кібербезпеці. Переважна більшість респондентів бачать ситуацію зовсім інакше. Коли їх запитали, в якій частині програми захисту їхньої організації виникли проблеми, пов’язані зі штучним інтелектом, відповіді стосувались ключових функцій кібербезпеки. Крім того, що управління інвентаризацією ІТ-активів назвали головною проблемною областю штучного інтелекту, інші три категорії кібербезпеки також потрапили до цього переліку згідно 53% респондентів:

- виявлення загроз (33%);

- розуміння сильних сторін і недоліків кібербезпеки (24%);
- оцінка ризиків порушення безпеки (23%);
- реагування на інциденти (13%).

Міф №3: штучний інтелект розумний, тому він має бути ефективним.

Очевидно, що хоча ШІ вже використовується в кібербезпеці, результати неоднозначні. Велика брехня полягає в тому, що не весь штучний інтелект є таким «розумним», як випливає з назви, і це навіть без урахування відповідності потребам і можливостям організації.

Штучний інтелект є сьогодні одним з трендів. Одним із популярних варіантів застосування ШІ в кібербезпеці розглядають GPT (Generative Pre-trained Transformer - мовні моделі машинного навчання, розроблені OpenAI, дослідницькою лабораторією та компанією, що базується в Сан-Франциско) – тип штучних нейронних мереж, які були натреновані на великих обсягах текстових даних з метою автоматичної генерації тексту.

1. GPT використовує архітектуру Transformer, що дозволяє моделі уважно аналізувати контекст тексту та генерувати зрозумілі та логічні продовження тексту.
2. GPT може бути використаний для виявлення шкідливого програмного забезпечення та зловмисних атак.
3. Використання GPT для аналізу поведінки користувачів може допомогти виявити потенційних зловмисників та запобігти кібератакам.
4. GPT може бути застосований для розпізнавання фішингових атак та інших спроб шахрайства в Інтернеті.
5. Застосування GPT для моніторингу соціальних мереж та форумів може допомогти виявити загрози для кібербезпеки.
6. Використання GPT для розпізнавання текстового контенту може допомогти виявити та відфільтрувати небажаний вміст, що містить загрози для безпеки.
7. GPT може бути використаний для побудови систем ідентифікації та аутентифікації користувачів, що забезпечує підвищену безпеку в мережах.
8. Застосування GPT для аналізу логів систем може допомогти виявити аномальну поведінку користувачів та зловмисних атак.
9. Використання GPT для розпізнавання мови та культур може допомогти виявити загрози, що виникають з-за міжкультурної спілкування.

Розгортаючи ШІ та оцінюючи рішення, організації повинні робити це зважено та орієнтуватися на результати ШІ. Якщо команди SOC не об’єднають штучний інтелект з досвідченими експертами, які знають технологію, вони ризикують зазнати невдачі у критичній галузі, яка практично не дає права на помилку.

Засновник новаторських високотехнологічних компаній Tesla та SpaceX Ілон Маск ще у 2018 році під час конференції South by Southwest в Остіні (Техас, США) жбурнув у маси пророчо-ексцентричну тезу про те, що штучний інтелект (AI) є небезпечнішим за ядерну зброю [55].

Уже стало ясно, що ризики від безконтрольного чи неетичного застосування технологій штучного інтелекту становлять цілком реальні небезпеки для людства. А саме:

- втрата робочих місць людьми через автоматизацію рутинних повторюваних операцій;
- порушення приватності, ледь не до повної її руйнації;
- Deepfakes («синтез слів «глибинне навчання» та «підробка» – методика синтезу зображення чи аудіоряду мовлення людини, яка базується на штучному інтелекті; вона використовується для поєднання і накладення наявних зображень та відео на вихідні зображення або відеоролики»;
- автоматизована зброя, що буде влучати у живі об'єкти без втручання людей-операторів;
- помилково-упереджені рішення систем через викривленість початкових навчальних даних (algorithmic bias);
- консервування соціально-економічної нерівності між різними верствами населення й націями в світі.

Таким чином, підсумовуючи, цивілізація за рахунок тотального застосування штучного інтелекту у всіх сферах людсьвої діяльності може перетворитися у:

- суспільство тотального контролю (хтось міг би назвати його ультраіндустріальним суспільством), в якому «деміурги», озброєні засобами систем штучного інтелекту, отримають можливість на кожному регулювати життя більшості людей.

- суспільство творців, де системи штучного інтелекту допоможуть людям звільнитися від рутини, відчути солідарність та спрямувати свій вільний час на творчу діяльність.

 *Питання для самоконтролю*:

1. Які можливі шляхи застосування штучного інтелекту в кібербезпеці?
2. Які існують міфи про застосування штучного інтелекту у кібербезпеці?
3. В чому полягає набезпека застосування штутчного інтелекту?
4. Які етичні проблеми застосування штучного інтелекту, в тому числі і в кібербезпеці?

 *Завдання:*

1. Знайти приклад застосування штучного інтелекту в кібербезпеці та розкрити його суть.
2. Створити алгоритм для перевірки вразливості внутрішньої компютерної мереж організації.

2.5. Професійні і корпоративні етичні кодекси в кібербезпеці

Однією з форм, що регулює принципи та правила ділової поведінки у міжнародній фірмі, організації, стали етичні кодекси, або кодекси поведінки. Сучасні умови соціально-економічного та науково-технічного перетворення у сфері ринкових відносин вимагають втілення нових ціннісних підходів до системи управлінських взаємовідносин, спрямованих на стратегічне управління людськими ресурсами.

Зміна ціннісних орієнтацій людства принесла радикальні зміни в етичну теорію й особливо в її прикладний аспект. Мінливість ділового середовища створила нагальну необхідність у комунікаціях зі співробітниками, партнерами, споживачами, що сприяло формуванню професійної та корпоративної етики як сукупності моральних норм, які визначають ставлення людини до професіонального обов’язку та цінностей організації [55].

Інтерес до феномену корпоративної етики зумовлений насамперед впливом етики та культури на життя організації, її положення у зовнішньому

світі, що, своєю чергою, відіграє неабияку роль у мобілізації ресурсів організації, необхідних для досягнення поставлених завдань, адже успішність будь-якої організації або колективу зумовлена різноманітними факторами, де однією з домінант виступає формування корпоративної етики організації [55-57].

Загалом на проблему взаємозв'язку моральних вимог та суспільної праці звертали увагу різні мислителі, такі як давньогрецький філософ Аристотель, шотландський філософ-моралість А. Сміт («Дослідження природи та причин багатства народів»). Пізніше – французький філософ О. Конт, соціолог і філософ Е. Дюркгейм, які також наголошували на взаємозв'язку суспільної праці з моральними принципами [58].

Незважаючи на те, що дотримання моральних норм підтримується лише силою суспільної дії, їх наявність необхідна ще й тому, що історично на основі норм моралі виробляються нові й удосконалюються існуючі юридичні норми, які забезпечуються силою державного впливу. На основі етичних стандартів, Міжнародна федерація з обробки інформації (IFIP – International Federation for Information Processing) рекомендувала прийняти кодекси комп'ютерної етики країн із врахуванням національних, культурних і етичних традицій.

Вперше, за участю Jisc (Joint Information Systems Committee, Спільний комітет інформаційних систем – британське агентство з цифрових технологій, даних та технологій, орієнтоване на вищу освіту, дослідження та інновації) був створений кодекс етики для всіх професіоналів, які працюють у групах реагування на інциденти з продуктами та комп'ютерною безпекою (PCIRTs та CSIRTs) у всіх секторах, включаючи освіту та дослідження.

PCIRT та CSIRT є абревіатурами, які використовуються в галузі кібербезпеки і пов'язані зі збором, аналізом та реагуванням на кіберінциденти в організаціях.

PCIRT – це скорочення від "Product or Production Computer Incident Response Team". Це команда фахівців з кібербезпеки, яка спеціалізується на реагуванні на інциденти, що стосуються продукту або виробництва. Такі команди зазвичай працюють в технічній підтримці виробника програмного забезпечення або апаратного забезпечення, тому їхній головний фокус – це забезпечення безпеки продукту або виробництва, а не безпеки організації, що використовує цей продукт.

CSIRT – це скорочення від "Computer Security Incident Response Team". Це команда фахівців з кібербезпеки, яка забезпечує реагування на кіберінциденти в

організації. Завданням CSIRT є швидке виявлення, аналіз та реагування на кібератаки та інші кіберінциденти, що можуть загрожувати безпеці організації та її інформаційних систем. CSIRT може бути внутрішнім (тобто створеним усередині організації) або зовнішнім (наприклад, організацією-постачальником послуг з кібербезпеки).

Кібербезпека та важлива робота груп реагування на інциденти безпеки у забезпеченні безпеки Інтернету ніколи не були настільки важливими, і зі зміною ландшафту безпеки сьогодні очікується багато від експертів, які працюють у цій галузі [55].

Як провідна організація та визнаний світовий лідер у реагуванні на інциденти, FIRST (Forum of Incident Response and Security Teams – Форум груп реагування на інциденти та безпеки) в рамках Агентства Європейського Союзу з кібербезпеки (European Union Agency for Cybersecurity – ENISA) функціонує подібно до професійної асоціації для членів CSIRT та PSIRT, а також інших фахівців з кібербезпеки з підготовкою та досвідом, пов'язаним з роботою команд реагування на інциденти та безпеки.

FIRST є провідною організацією та визнаним світовим лідером у реагуванні на інциденти. Членство в FIRST дозволяє групам реагування на інциденти більш ефективно реагувати на інциденти безпеки реактивними, а також проактивними. FIRST об'єднує різноманітні групи реагування на інциденти комп'ютерної безпеки з урядових, комерційних та освітніх організацій. FIRST має на меті сприяти співпраці та координації у запобіганні інцидентам, стимулювати швидке реагування на інциденти та сприяти обміну інформацією між членами та громадою в цілому. На даний час FIRST налічує понад 600 членів, поширених по Африка, Америці, Азії, Європі та Океанії.

Світ навколо FIRST все більше усвідомлює важливість питань кібербезпеки та важливої роботи груп реагування на інциденти безпеки для забезпечення безпеки та надійності Інтернету. Як наслідок, від SIRTs очікується все більше і більше заходів та зусиль, і все більше і більше виникає питань щодо належної ролі та очікуваної поведінки SIRT. На ці питання потенційно може відповісти остаточний набір тверджень про те, що SIRTs будуть або не будуть робити у Першому кодексі етики кібербезпеки.

Новий кодекс етики для фахівців з кібербезпеки EthicsfIRST – це керівні принципи, що застосовуються для всіх секторів, включаючи європейські NREN (National Research and Education Networks – Національні науково-освітні мережі).

EthicsfIRST (Ethics for Incident Response and Security Teams – Етика для команд реагування на інциденти та безпеки) – має на меті надати практичні поради та підтримку спільноті CSIRT, у тому числі серед європейських учасників. Створені Форумом груп реагування на інциденти та безпеки за допомогою керівника оперативного центру безпеки Jisc, доктора Джона Чепмена, нові керівні принципи тепер видані для консультацій. Кодекс розроблений, щоб керувати етичною поведінкою всіх членів команди, які ефективно використовують кібербезпеку. Заяви про відповідальність засновані на розумінні того, що суспільне благо завжди є першочерговим розглядом. Ці заяви спрямовані на посилення обов'язків щодо надійності, скоординованого розкриття вразливостей, авторизації, здоров'я команди та визнання меж юрисдикції.

Доктор Чепмен, який брав участь у розробці нового кодексу в рамках своєї ролі в групі спеціальних інтересів з етики FIRST, сказав: «Оскільки фахівці з безпеки піднімаються до виклику технологічних змін і загроз, що розвиваються, те, як вони приймають рішення щодо обробки інцидентів, може викликати етичні питання. Окремі професійні органи, такі як ISACA[50] або BCS[51], мають власні кодекси для членів, але кодекс етики FIRST – це всеохоплюючий, міжгалузевий документ, який є актуальним для всіх. Обидві організації є авторитетними в галузі інформаційної безпеки та управління технологіями і здійснюють різноманітні діяльності, такі як розробка стандартів, проведення навчальних курсів, сертифікація фахівців та проведення конференцій. Кодекс EthicsfIRST буде у вільному доступі для будь-якої організації, і я, безумовно, буду заохочувати членів Jisc, які керують власними CSIRT, прийняти його. Я сподіваюся, що, застосувавши EthicsfIRST на практиці, це допоможе зміцнити довіру між командами та між командами та їхніми спільнотами. Керівні принципи EthicsfIRST дають фахівцям з безпеки та командам впевненість у тому, що вони краще справляються методично зі складними етичними ситуаціями. Це великий крок вперед у подальшій професіоналізації фахівців з безпеки».

Кодекс Етики FIRST. Етика груп реагування на інциденти та безпеки

[50] ISACA (англ. Information Systems Audit and Control Association) є глобальною організацією, яка займається розробкою та підтримкою стандартів, засобів і практик у галузі управління технологіями та інформаційної безпеки. Члени ISACA можуть бути керівниками інформаційної безпеки, аудиторами, консультантами та іншими фахівцями, які працюють у галузі інформаційних технологій та безпеки.

[51] BCS (англ. British Computer Society) є професійною організацією, яка займається розвитком та підтримкою стандартів інформаційної технології, управління проектами, бізнес-аналітики та інших суміжних галузей. BCS виконує функції асоціації фахівців з інформаційних технологій та надає своїм членам можливості для професійного розвитку, сертифікації та мережевого взаємодії.

Члени команд реагування на інциденти та безпеки (Teams) мають доступ до багатьох цифрових систем та джерел інформації. Їх дії можуть змінити світ. Як член цієї професії, член команди повинен визнати відповідальність перед своїм виборчим округом та іншими фахівцями з безпеки, а також перед суспільством у цілому. Індивід також повинен визнати свою відповідальність перед власним благополуччям.

EthicsfIRST розроблений, щоб надихати та керувати етичною поведінкою всіх членів команди, включаючи поточних та потенційних практиків, викладачів, студентів, впливових осіб та всіх, хто використовує обчислювальні технології впливовим чином. Ця структура включає в себе принципи, сформульовані як заяви про відповідальність, засновані на розумінні того, що суспільне благо завжди є першочерговим фактором. Кожен принцип доповнюється керівними принципами, які надають пояснення, щоб допомогти фахівцям з обчислювальної техніки зрозуміти і застосувати принцип. Основні принципи цього кодексу в Додатку Г.

Ці обов'язки слід розглядати не як абсолютні вимоги, а скоріше, як зазначено в IETF RFC2119[52], для визначення «ПОВИНЕН»: "Це слово, або прикметник "РЕКОМЕНДОВАНО", означає, що в конкретних обставинах можуть існувати поважні причини для ігнорування конкретних обов'язків, але всі наслідки повинні бути зрозумілі та ретельно зважені, перш ніж вибрати інший курс". Наприклад, члени команди часто можуть опинитися в положенні, коли жодна дія, здається, не задовольняє всім етичним принципам. У такій ситуації необхідно зробити вибір щодо того, які розставити пріоритети. У цій ситуації обробникам інцидентів рекомендується подумати про те, які і як зацікавлені сторони можуть постраждати від їхніх дій, але бажано в дискусії з колегою. Як правило, слід вибирати рішення, яке мінімізує порушення цих етичних рамок. Іноді це може бути неможливим, наприклад, через зовнішній тиск. У такій ситуації рекомендується діяти, відзначаючи етичну дилему, можливо, під знаком протесту.

Обов'язок благонадійності. Довіра є основою багатьох відносин між Teams і часто вимагається для розуміння того, як може відбутися змістовний обмін інформацією. Спільнота FIRST побудована на цій довірі, і вона може

[52] IETF RFC2119 - це стандарт, який визначає ключові слова та фрази, що використовуються в документах Інженерної робочої групи Інтернету (IETF) для визначення рівня вимог до реалізації протоколів та інших стандартів.

продовжувати функціонувати таким чином лише за умови розумного рівня довіри між командами.

Надійність означає, що члени команди повинні лише:

1) брати на себе зобов'язання, які вони можуть дотримуватися;

2) поводитися передбачувано по відношенню до інших Команд (наприклад, поважати стандарт TLP[53]);

3) підтримувати довірчі відносини, які вони мають з іншими Командами.

Довірчі відносини повинні бути спочатку передбачуваними і транзитивними, тобто Trust on First Use (TOFU), і забезпечувати довіру для Команд, яким довіряють інші Команди.

Обов'язок скоординованого розкриття вразливостей. Члени команди, які дізнаються про вразливість, повинні стежити за скоординованим розкриттям вразливостей, співпрацюючи із зацікавленими сторонами для усунення вразливості безпеки та мінімізації шкоди, пов'язаної з розкриттям інформації. Зацікавлені сторони включають репортера вразливостей, постраждалих постачальників, координаторів, захисників та клієнтів, партнерів та користувачів, але не обмежуються ними.

Члени команди повинні координувати свої дії з відповідними зацікавленими сторонами, щоб узгодити чіткі терміни та очікування щодо оприлюднення інформації, надаючи достатньо деталей, щоб користувачі могли оцінити свій ризик та вжити дієвих захисних заходів.

Обов'язок дотримання конфіденційності. Члени команди зобов'язані зберігати конфіденційність, де це доречно. Запити на збереження певної інформації в таємниці можуть бути явними, наприклад, за допомогою протоколу світлофора (TLP). Члени команди повинні поважати такі прохання, коли це можливо. Якщо неможливо зберегти інформацію в таємниці, наприклад, через конфлікт з вимогами місцевих законів, контрактів або обов'язком інформувати, член Команди повинен негайно повідомити власника інформації про цей конфлікт.

Деякі обов'язки щодо конфіденційності ґрунтуються на законах, нормативних актах або звичаях. Якщо під час реагування на інцидент деякі сторони пов'язані або очікують конфіденційності на основі таких міркувань,

[53] Протокол світлофора (TLP) - це система класифікації конфіденційної інформації, створена на початку 2000-х років Координаційним центром національної безпеки інфраструктури уряду Великобританії (NISCC; зараз Центр захисту національної інфраструктури, CPNI) для заохочення більшого обміну конфіденційною інформацією. Основна концепція полягає в тому, щоб оригінатор сигналізував, наскільки широко вони хочуть, щоб їх інформація поширювалася за межами безпосереднього одержувача.

вони повинні зробити все можливе, щоб ці очікування були явними заздалегідь. Після цього всі сторони повинні дотримуватися вищезазначених очікувань щодо підтримки явних запитів на збереження інформації в таємниці, коли це можливо.

Обов'язок визнати. Команди отримують інформацію з багатьох різних джерел: дослідників, клієнтів, інших команд, державних установ тощо. Члени команди повинні своєчасно відповідати на запити, навіть якщо це тільки для підтвердження того, що запит був отриманий. Коли це можливо, члени команди повинні встановити очікування щодо наступного оновлення.

Обов'язок авторизації. Члени команди мають законну потребу і право розуміти свої зони відповідальності, діючи тільки в системах, до яких вони уповноважені на доступ. Члени команди повинні усвідомлювати, як їх дії можуть вплинути на складові систем, і стежити за тим, щоб вони не завдавали додаткової шкоди під час виконання своїх обов'язків. Там, де це можливо, слід проконсультуватися зі знавцями перед внесенням змін до їхніх систем.

Обов'язок інформувати. Члени команди повинні вважати своїм обов'язком інформувати своїх учасників про поточні загрози та ризики безпеки. Коли члени команди мають інформацію, яка може негативно вплинути або покращити безпеку та захист, вони зобов'язані інформувати відповідні сторони або інших осіб, які можуть допомогти, докладаючи відповідних зусиль, належним чином враховуючи конфіденційність, закони та правила щодо конфіденційності та інші зобов'язання.

Обов'язок поважати права людини. Члени команди повинні знати, що їхні дії можуть вплинути на права інших осіб через обмін інформацією, можливе упередження в їхніх діях або порушення прав власності. Члени команди мають доступ до широкого спектру особистої, конфіденційної та конфіденційної інформації під час розгляду інцидентів. Ця інформація повинна оброблятися таким чином, щоб відстоювати права людини.

Під час обробки інцидентів реагувальники не повинні діяти упереджено і повинні робити все можливе, щоб усунути упередженість у своїх процесах та прийнятті рішень, чи виконуваних відповідачами, чи вбудованих в алгоритми.

Для цілей цього принципу поняття «власність» (Декларація прав людини ООН: стаття 17) включає в себе нематеріальні активи, такі як інтелектуальна власність, а також ідеї та концепції в цілому, незалежно від того, чи охороняються вони законом (наприклад, запатентовані).

Обов'язок перед здоров'ям команди. Команди несуть відповідальність за продовження надання послуг, які вони пообіцяли своїм учасникам. Ця відповідальність включає фізичне та емоційне здоров'я команди.

Для того, щоб поважати як особистість членів, які складають команду, так і забезпечувати довгострокову життєздатність підтримки належного рівня обслуговування, команда повинна прагнути підтримувати здорове, безпечне та позитивне робоче середовище, яке забезпечить фізичне та емоційне здоров'я (всіх) її членів. Для того щоб відреагувати на кризу, «нормальні» операції повинні підтримувати емоційне здоров'я і зниження стресу.

Обов'язок перед командними здібностями. Управління інцидентами - це тема, що розвивається, яку члени команди повинні постійно вивчати. Команда повинна надавати ресурси своїм членам для вивчення, застосування та просування технологічних і наукових знань у межах своєї сфери (областей) відповідальності. Навчальні або освітні кредити можуть сприяти, але простих вправ на відповідність вимогам недостатньо для виконання цього обов'язку. Команда повинна підтримувати достатню технологічну інфраструктуру таким чином, щоб забезпечити надання своїх послуг, включаючи адекватні заходи для захисту цієї інфраструктури від втручання сторонніх сторін.

Обов'язок по відповідальному стягненню. Збір даних необхідний для реагування на інциденти, але слід дотримуватися балансу між метою реагування на інциденти та повагою до зацікавлених сторін.

Під час розслідування обсяг інформації, необхідної для збору, може змінюватися. Аналізуючи інцидент, члени команди повинні коригувати те, що вони збирають, коли потреба змінюється. Дані, які безпосередньо не стосуються інциденту, та їх виправлення повинні бути виключені зі звітування.

Зібрані та вилучені дані повинні оброблятися відповідно до чинного законодавства та поваги до конфіденційності користувачів. Слід шукати дозвіл перед збором та обробкою даних під контролем власника даних. Слід дотримуватися чинного законодавства та нормативно-правових актів у поводженні з даними.

Дані, які можуть допомогти іншим групам реагування в їхніх зусиллях, пов'язаних з іншими інцидентами, повинні бути доступні їм, можливо, у відредагованій формі. Інформація, яка є конфіденційною, повинна бути доступна лише з відповідним захистом.

Перш ніж ділитися даними з третіми сторонами для пом'якшення ризиків слід зважити на переваги. Даними слід ділитися лише в тому випадку, якщо вигода явно переважає ризики. Конфіденційні дані повинні зберігатися таким чином, щоб їх можна було легко знищити після закриття інциденту. Зібрані дані повинні бути безпечно знищені відповідно до політики збереження даних.

Обов'язок визнавати юрисдикційні межі. Члени команди повинні визнавати та поважати межі юрисдикції, законні права, правила та повноваження сторін, які беруть участь у діяльності, пов'язаній з реагуванням на інциденти.

Закони, нормативні акти та інші юридичні питання, такі як ті, що стосуються захисту конфіденційності або повідомлень про порушення даних, можуть відрізнятися між відповідними юрисдикціями. Юрисдикційні межі можуть визначатися фізичним розташуванням залучених сторін, такими як їхні країни або місця проживання, а також іншими факторами, що стосуються цих сторін. Навіть в межах однієї країни закони та правила можуть відрізнятися між політичними регіонами (наприклад, між окремими штатами в США) або між різними підприємствами, галузями чи секторами в цій країні (наприклад, охорона здоров'я, фінансові послуги та державні установи). Національні CSIRT можуть мати визначені обов'язки та/або повноваження щодо діяльності, що стосується складових у межах їх власної юрисдикції, а також вони можуть співпрацювати або «передавати» інформацію та діяльність іншим організаціям, які мають повноваження для юрисдикцій, які перетинають кордони.

Члени команди повинні знати про ключові проблеми, які впливають на залучені юрисдикції, включаючи, але не обмежуючись ними, правила конфіденційності або вимоги щодо сповіщення про порушення даних. Оскільки закони та правила про кібербезпеку та конфіденційність розвиваються та продовжують оновлюватися в усьому світі, доцільно проконсультуватися з поінформованим юридичним радником для отримання вказівок, коли проблеми пов'язані з кількома межами юрисдикції.

Обов'язок доказової аргументації. Команди повинні діяти на основі фактів, що перевіряються. Під час обміну інформацією, такою як індикатори компрометації або описи інцидентів, члени команди повинні прозоро надавати докази та обсяг інформації. Якщо це неможливо, слід навести причини ненадання цих доказів та обсягу інформації.

Члени команди повинні утримуватися від поширення чуток. Будь-яка гіпотеза повинна бути чітко ідентифікована як така. Прозорі процеси доказів та

міркувань важливі навіть у випадку автоматизованого обміну, наприклад, під час автоматизованого обміну великих обсягів інформації. При цьому опис процесу інтелектуального аналізу даних має бути повідомлено на зрозумілому рівні деталізації.

Нижче наведено кілька визначних прикладів етичних кодексів для ІТ-фахівців:

1. RFC 1087/ У січні 1989 року Рада архітектури Інтернету (IAB) у RFC 1087 визначає діяльність як неетичну та неприйнятну, якщо вона:

- прагне отримати несанкціонований доступ до ресурсів Інтернету;
- руйнує цілісність комп'ютерної інформації;
- порушує конфіденційність користувачів.

2. Кодекс чесної інформаційної практики заснований на п'яти принципах, що викладають вимоги до систем ведення документації.

- не повинно бути систем обліку персональних даних, існування яких є секретним.
- для особи має бути спосіб дізнатися, яка інформація про особу міститься в записі та як вона використовується.
- для особи має існувати спосіб запобігти використанню інформації про особу, яка була отримана з однією метою, чи доступу для інших цілей без її згоди.
- для особи має бути спосіб виправити або змінити запис ідентифікаційної інформації про особу.
- будь-яка організація, яка створює, веде, використовує або розповсюджує записи ідентифікаційних персональних даних, повинна гарантувати надійність даних для їх передбачуваного використання та вжити заходів для запобігання неправомірному використанню даних. Ця вимога була реалізована в 1973 році Міністерством охорони здоров'я, освіти та соціального забезпечення США.

Питання для самоконтролю:

1.З чого складається професійний етичний кодекс?

2.В чому відмінність між професійним та корпоративним кодексами?

3.В чому особливість корпоративних кодексів кібербезпеки?

4.Які функції виконують корпоративні кодекси кібербезпеки?

Завдання:

1. Зробити аналіз та виявити відмінності між EthicsfIRST та кодексами у Додатку А в кінці посібника.
2. Зробити аналіз кодексу Асоціації безпеки інформаційних систем (ISSA) за посиланням: https://cdn.ymaws.com/www.members.issa.org/resource/resmgr/docs/issa_ethics_review_policy_-_.pdf

2.6. Особливості впровадження кодексів корпоративної етики у провідних компаніях світу та в Україні

Кодекси корпоративної етики є невід'ємною частиною сучасної бізнес-культури. Вони стали інструментом, що дозволяє компаніям забезпечувати етичне поводження своїх співробітників, підвищувати репутацію та залучати талановитих працівників і підвищувати конкурентоспроможність.

Корпоративна етика – явище досить нове.

Про нього стали говорити тільки з того моменту, коли в різних галузях господарської та соціальної діяльності стали домінувати великі компанії, влаштовані за принципом скрупульозного поділу праці.

Окремим випадком служать сучасні транснаціональні компанії, чия діяльність протікає в масштабах усього світу. Із цього погляду метою корпоративної етики можна вважати не стільки збереження високих стандартів професії, як саме формування єдиного корпоративного духу в ситуації, коли деякі складові частини компанії розкидані в різних частинах світу.

Корпоративна етика, орієнтуючи на універсальні моральні принципи (насамперед принципи справедливості: рівність людських прав і повагу гідності людської істоти як індивідуальної особистості; принцип благоговіння перед життям), формує певний рівень морального розвитку як окремої особистості, так і організації в цілому [59].

Таке поняття, як «кодекс етики», або «етичний кодекс», з'явилося дуже давно й існує вже доволі довгий час. Такі кодекси лежать в основі багатьох релігійних традицій та культур. Наприклад, кодекс Десяти Заповідей є священним і основоположним для іудаїзму, ісламу та християнства.

Сьогодні ж кодекси корпоративної або професійної етики набули більш модернового вигляду і зазвичай подаються у вигляді конкретного документа з визначеними пунктами і чіткими правилами поведінки. Кожна солідна компанія керується у свої діяльності такими кодексами, чого вимагає і від своїх працівників.

Один із найпоширеніших кодексів корпоративної етики у світі - це Кодекс Європейської комісії з етики в галузі досліджень (European Commission Code of Conduct for Research Integrity). Цей кодекс розроблений з метою забезпечення етичної поведінки учасників дослідницької діяльності, зокрема, науковців, університетів та наукових установ. Він охоплює широкий спектр питань, від поведінки під час виконання досліджень до публікації наукових робіт.

Ще один поширений кодекс корпоративної етики - це Кодекс поведінки для банківської системи США (Code of Conduct for the U.S. Banking System). Цей кодекс містить рекомендації щодо етичної поведінки банківських установ та працівників банків, включаючи запобігання конфлікту інтересів, забезпечення безпеки та конфіденційності даних клієнтів та уникнення недобросовісної конкуренції.

Еталонними у складанні кодексів корпоративної етики вважаються японські компанії. Кодекс поведінки співробітників японських компаній включає кілька груп критеріїв (табл. 2.1) [60].

Таблиця 2.1

Критерії поведінки співробітників японських компаній

Ставлення до компанії	**Ставлення до роботи**	**Ставлення до старших, колег та підлеглих**	**Ставлення до себе**
Відданість	Старанність	Вміння працювати у команді	Догляд за здоров'ям
Вдячність	Відповідальність, виконання обов'язків	Приязнь і чемність	Бадьорість
–	Ощадливість, акуратність, терплячість	–	Моральна стійкість

Ставлення до компанії	Ставлення до роботи	Ставлення до старших, колег та підлеглих	Ставлення до себе
–	Почуття гордості за свою роботу	–	–

Серед інших компаній, які ставлять корпоративну етику не на останнє місце в управлінні компанією і розробили відмінні зразки кодексів корпоративної етики і поведінки, можна виділити The Coca-Cola Company, Starbucks, Pepsi Co, IKEA, Facebook, Microsoft, Johnson&Johnson, Procter&Gamble, Unilever, IBM, General Motors, Nokia та ін.

Особливістю кодексу корпоративної етики Google є те, що його легко читати. Не потрібна юридична освіта, щоб зрозуміти, що має на увазі компанія. Також його легко знайти онлайн. В наявності посилання на різні розділи, а надані відповіді – ретельні та докладні. Коексмістить багато етичних питань, які слід розглянути, такі як помста, конфлікти інтересів, хабарництво та конфіденційність.

Україна відноситься до країн, де впровадження кодексів корпоративної етики є актуальним питанням. Основна мета впровадження кодексів корпоративної етики в Україні полягає у забезпеченні високих стандартів етики та прозорості в управлінні компанією. Це дозволяє збільшити довіру споживачів та інвесторів до компанії та підвищити її конкурентоспроможність на ринку.

Так, один із найбільших банків України – «ПриватБанк» у своєму кодексі виокремлює такі положення: «Ми готові звернути гори, щоб гарно обслуговувати клієнта. Якщо ми не можемо цього зробити самі, то залучаємо інших співробітників – аж до Голови правління банку»; «ми посміхаємося нашим клієнтам. Робимо це щиро і якнайчастіше, адже ми вдячні їм за те, що вони наші клієнти!»; «ми обслуговуємо клієнта так, як хотіли б, щоб обслуговували нас або нашу маму». Про ставлення до колег, роботи та банку у цілому: «Ми працюємо більше, ніж співробітники інших банків, але ми й заробляємо більше»; «ми позитивні люди. Ми посміхаємося оточуючим. Загалом із нами приємно мати справу» [61].

На відміну від «ПриватБанку», кодекс якого – це кілька пунктів, кодекс НАК «Нафтогаз» – це повноцінний PDF-документ обсягом 56 сторінок. У ньому прописані загальні правила корпоративної етики компанії, розділені на групи: корпоративні цінності, політика у різних сферах життєдіяльності, політика щодо

захисту інформації, політика щодо подарунків і гостинності, відповідальність за дотримання положень кодексу – загалом 21 пункт [62].

Медіагігант «1+1 Медіа» не має чітко окресленого набору правил корпоративної етики, однак на офіційному сайті представлено основні принципи, яких дотримується компанія у своїй діяльності. До них належать: чисте довкілля, якісна освіта, здорова нація, повага до авторських прав, звітність та можливість зворотного зв'язку [63].

Більшість великих компаній вже мають свої власні кодекси, але їх виконання не завжди є повним та ефективним. Однією з причин такої ситуації є недостатня увага до процесу впровадження та практичного застосування кодексів. Впровадження та практичне застосування цих кодексів може стикатися з різними проблемами та перешкодами.

Це може бути:

1.Недостатній контроль за виконанням кодексів корпоративної етики.

Однією з основних проблем впровадження кодексів корпоративної етики в Україні є відсутність достатнього контролю за їх виконанням. Багато компаній не приділяють достатньо уваги процесу виконання своїх кодексів, що може призводити до порушень в етичній поведінці працівників та зниження довіри до компанії. Особливо це стосується маленьких та середніх підприємств, які можуть не мати достатньої кількості ресурсів для забезпечення контролю за виконанням своїх кодексів.

Для вирішення цієї проблеми, компанії повинні створювати механізми контролю за виконанням своїх кодексів та забезпечувати їх регулярне оновлення та адаптацію до змін у законодавстві та етичних стандартах.

2.Недостатня освіченість та усвідомлення значення корпоративної етики.

Іншою проблемою впровадження кодексів корпоративної етики є недостатня освіченість працівників щодо їх значення та важливості. Це може призводити до того, що працівники не розуміють необхідності дотримання корпоративної етики та не бачать її впливу на успішність компанії.

Для вирішення цієї проблеми, компанії повинні проводити регулярні навчання та тренінги для своїх працівників щодо корпоративної етики та наголошувати про її важливість для успішної роботи компанії. Також важливо створити культуру, де дотримання корпоративної етики є нормою, а не винятком.

3.Низький рівень правової культури та недостатнє законодавство.

Ще однією проблемою впровадження кодексів корпоративної етики в Україні є низький рівень правової культури та недостатнє законодавство щодо цієї теми. Українське законодавство не містить достатньої кількості норм, які б забезпечували відповідальність за порушення корпоративної етики, тому виконання кодексів може бути невідчутним для компаній та їх працівників.

Для вирішення цієї проблеми, необхідно вдосконалити законодавство та включити до нього норми щодо відповідальності за порушення корпоративної етики. Також важливо підвищити рівень правової культури серед працівників та населення загалом, щоб збільшити свідомість щодо необхідності дотримання етичних стандартів.

4.Невідповідність між кодексом та реальною практикою.

Останньою проблемою впровадження кодексів корпоративної етики в Україні є невідповідність між кодексом та реальною практикою в компаніях. Це може бути пов'язано зі звичайними практиками, які виконуються у компанії, але не відповідають етичним стандартам, встановленим у кодексі.

Для вирішення цієї проблеми, компанії повинні забезпечувати контроль за виконанням кодексу та практиками, що використовуються в компанії. Також необхідно створити процедури, які б допомагали виявляти порушення кодексу та вживати заходів для їх усунення.

Висновок. Отже, кодекс корпоративної етики є важливим інструментом для забезпечення етичної поведінки компаній та їх працівників. Проте, впровадження кодексу в Україні зіткнулося зі значними проблемами, такими як недостатня увага до етики в бізнесі, низький рівень правової культури та невідповідність між кодексом та реальною практикою. Для розв'язання цих проблем необхідно проводити навчання та тренінги для працівників, вдосконалювати законодавство та забезпечувати контроль за виконанням кодексу та етичними стандартами в компанії. Тільки так можна досягти повного впровадження корпоративної етики в Україні та забезпечити успішну роботу компаній у майбутньому.

 *Питання для самоконтролю*:

1.Коли і ким був створений перший корпоративний кодекс?

2.Які корпоративні кодекси є в Україні та чим вони відрізняються від західноєвропейських компаній?

3.В чому суть управлінської функції корпоративного кодексу?

Завдання:

1. Зробити аналіз корпоративних кодексів Приватбанку та Нафтогазу.
2. Розібрати зміст корпоративного кодексу GOOGLE.

Розділ 3
ЕТИКА КОНФЛІКТІВ В КІБЕРБЕЗПЕЦІ

3.1. Види конфліктів, їх сутність та методи вивчення і способи розв’язання

Термін "конфлікт" має безліч різних визначень. В управлінській науці конфлікт розглядається як відсутність згоди між двома або більше сторонами. Суб'єктами конфлікту можуть бути окремі люди, малі групи, або цілі колективи.

У науковій літературі виділяються різні підходи до суті і оцінки конфлікту. З погляду авторів, що належать до школи наукового управління, заснованої на теорії бюрократії Вебера[54], конфлікт - негативне явище в управлінській діяльності. Конфліктів слід уникати, але якщо вони з'являються - вирішувати негайно. Даний підхід до конфлікту спирався на уявлення про організацію, як сукупність певних завдань, процедур, правил взаємодії посадових осіб і розробленої раціональної структури. Подібні механізми усувають умови для виникнення конфліктів і ведуть до безконфліктного розвязання проблем.

Автори, що належать до школи "людських відносин", також вважали, що конфлікту можна і необхідно уникати. Вони допускали можливість появи суперечностей між цілями окремих осіб і цілями організації, можливостями однієї особи і різними групами керівників і т.д. Але з погляду концепції "людських відносин" конфлікт є ознакою неефективної діяльності організації і поганого управління.

Сучасний підхід до суті конфлікту розглядає його як неминучий, і навіть в деяких випадках необхідний елемент діяльності організації. Нерідко конфлікт має негативний характер. Іноді він може заважати задоволенню потреб окремої особи і досягненню цілей організації в цілому. Але в багатьох ситуаціях конфлікт допомагає виявити різноманітність точок зору, дає додаткову інформацію, допомагає виявити більше число альтернатив або проблем. Це робить процес ухвалення рішення ефективнішим, а також дає можливість людям виразити свої думки, задовольнити свої особисті потреби в пошані і владі. Це також може привести до ефективнішого виконання планів, стратегій і проектів, оскільки

[54] Теорія бюрократії Макса Вебера - це концепція організації та управління, що базується на раціональній системі, яка використовується для досягнення максимальної ефективності та прозорості.

обговорення різних точок зору на ці документи під час розв’язання конфлікту відбувається до їх фактичного виконання.

Отже, конфлікт може бути функціональний і вести до підвищення ефективності в організації. Або він може бути дисфункціональним і призводить до зниження особистої задоволеності, групової співпраці і ефективності організації. Роль конфлікту залежить від того, наскільки ефективно ним управляють. Для управління конфліктом необхідно з'ясувати структуру конфлікту та виникнення конфліктної ситуації.

Один із варіантів структури конфлікту показаний науковцями [64] на рис.3.1 .

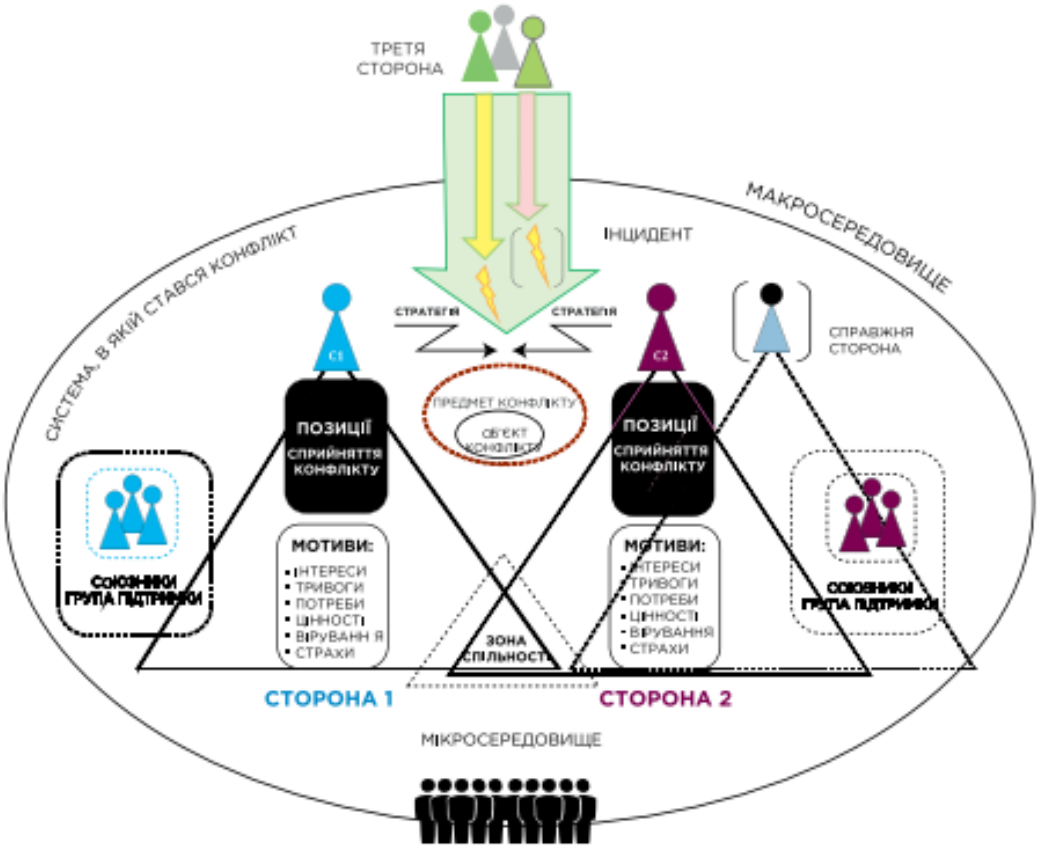


Рис. 3.1. Структура конфлікту

У практиці роботи управлінця (менеджера) постійно виникає необхідність у виборі різноманітних методів впливу на конфлікти і управління ними. Для їх ефективності важливо підбирати конкретні методи і форми залежно від того чи іншого виду конфлікту, а для цього необхідно вміти своєчасно визначати, до якого виду він відноситься.

Використовуючи ситуаційний підхід, є можливість економити ресурси, підвищувати оперативність прийняття управлінських рішень, що позитивно позначиться на ефективність управлінської діяльності.

Конфлікти розгортаються і згасають, розв’язуються чи трансформуються, однак у системах із тривалими соціальними зв’язками (колективи, команди, родини тощо) скріш за все будуть існувати цикли, коли конфлікт то згасає, то розгоряється знову. Якщо причина конфлікту не зникає, учасники залишаються в одній системі, відновлюють сили і продовжують конфліктувати, відтак через виснаження сторін конфлікт на якийсь час згасає, але потім все повторюється знову (рис. 3.2) [64].

Рис. 3.2. Циклічність фаз конфлікту

Для првильного планування роботи з усунення конфлікту та його рзвязання необхідно з самого початку визначити його причини.

Причини виникнення конфлікту - це явища, події, факти, ситуації, які передують конфлікту і, при визначених умовах діяльності суб'єктів соціальної взаємодії, спричинюють його. Серед великої кількості причин конфліктів передусім виділяють загальні причини, які так чи інакше проявляються практично в усіх виникаючих конфліктах. Їх розділяють на :

- соціально-політичні та економічні (пов'язані із соціальнополітичною ситуацією в країні);
- соціально-демографічні (відмінності в установках і мотивах людей, зумовлені їх статтю, віком, приналежністю до етнічних груп);
- соціально-психологічні (соціально-психологічні явища у групах: взаємовідносини, лідерство, групові мотиви тощо);

- індивідуально-психологічні (відображають індивідуальнопсихологічні особливості особистості: здібності, темперамент, характер, потреби тощо). Часткові причини безпосередньо пов'язані з конкретним видом конфлікту (порушення трудового законодавства, службової етики, незадоволеність умовами діяльності та ін.).

Конфлікти споконвічно виникають внаслідок порушення балансу інтересів двох і більше сторін. У зв'язку з цим виділяють об'єктивні і суб'єктивні причини конфліктів.

Об'єктивні причини конфліктів існують незалежно від волі і бажання учасників взаємодії (обмеженість у ресурсах, погані комунікації тощо). Основні з них [64]:

- обмеженість ресурсів, які треба ділити;
- взаємозалежність завдань;
- розбіжності в меті;
- розбіжності в уявленнях і цінностях;
- розбіжності у манері поведінки і життєвому досвіді;
- незадовільні комунікації

Розподіл ресурсів. Навіть у великих організаціях ресурси завжди обмежені. Керівництво повинне вирішити, як розподілити матеріали, людські ресурси, фінанси між різними групами, щоб найбільш ефективним способом досягнути вершини організації. Виділення значної частини ресурсів якомусь одному керівникові чи групі означає, що інші одержать меншу частку від загальної кількості. Таким чином, необхідність ділити ресурси майже безповоротно веде до різних видів конфліктів.

Взаємозалежність завдань. Можливість конфлікту існує всюди, де одна людина чи група залежить від іншої людини чи групи. Наприклад, керівник виробничого підрозділу може пояснити низьку продуктивність своїх підлеглих нездатністю ремонтної служби достатньо швидко ремонтувати обладнання. Керівник ремонтного підрозділу, в свою чергу, може звинувачувати кадрову службу, що не прийняла на роботу більш кваліфікованих працівників. Оскільки всі організації є системами, що складаються із взаємозалежних елементів, то при незадовільній роботі одного підрозділу чи людини взаємозалежність завдань може стати причиною конфлікту.

Розбіжності в меті. Можливість конфлікту збільшується в міру того, як організації стають більш спеціалізованими і розбиваються на окремі підрозділи.

Це відбувається тому, що спеціалізовані підрозділи самі формулюють свою мету і приділяють їм більше уваги, ніж меті організації. Наприклад, відділ збуту може наполягати на виробництві якомога більше різноманітної продукції тому, що це підвищує конкурентноздатність підприємства і збільшує обсяг збуту. У той же час цілі виробничого підрозділу більше спрямовані на валові обсяги і менше на асортимент продукції.

Розбіжності в уявленнях і цінностях. Уявлення про якусь ситуацію залежить від бажання досягнути певної мети. Замість того, щоб об'єктивно оцінити ситуацію, люди можуть дотримуватися тих поглядів, які, на їх думку, сприятливі для їх групи і особистих потреб. Ця тенденція була виявлена в одному дослідженні, де керівників різних відділів попрохали вирішити проблему, пов'язану з поліпшенням обслуговування клієнтів. Кожен керівник при цьому вважав, що проблему обслуговування клієнтів найкраще може вирішити тільки його функціональний підрозділ. Таким чином, у кожного з керівників були свої уявлення щодо вирішення цієї проблеми, які не збігалися з уявленнями інших керівників. Розбіжності у цінностях - також дуже розповсюджена причина конфлікту. Наприклад, підлеглий може вважати, що він завжди має право на висловлення своєї думки, у той час як керівник вважає, що підлеглий має право висловлювати свою думку лише тоді, коли його питають.

Ще приклад: персонал може цінувати свободу і незалежність. Якщо керівник уважно стежить за роботою своїх підлеглих, розбіжності в цінностях, вірогідно, спричинять конфлікт. Розбіжності у манері поведінки і життєвому досвіді можуть збільшити вірогідність виникнення конфлікту. Наприклад, люди, що постійно проявляють агресивність і ворожість і готові сперечатися за кожне слово, створюють навколо себе атмосферу, що може спричинити конфлікт. Дослідження показали, що розбіжності у життєвому досвіді, характері, віці, освіті зменшують ступінь взаєморозуміння та співробітництва між представниками різних підрозділів.

Незадовільні комунікації. Погана передача інформації є як причиною, так і наслідком конфлікту. Наприклад, якщо керівництво не може довести до відома підлеглих необхідність реорганізації виробництва, останні можуть відреагувати таким чином, що сповільнять темп роботи. Ці проблеми також можуть виникнути і посилитися через нездатність керівників розробити і довести до відома підлеглих точний опис посадових обов'язків. При цьому у будь-якому з підрозділів буде підґрунтя для утворення міжособистісних та інших конфліктів.

Суб'єктивні причини зумовлені передусім конкретною поведінкою індивіда та психологічною структурою особистості - характером, темпераментом, спрямованістю, ціннісними орієнтаціями, потребами тощо. Оскільки кожна людина як особистість багатогранна, суб'єктивні причини набувають різноманітних форм і видів. Вони проявляються як невідповідність цих факторів конкретній життєвій ситуації (продумати приклади зі соціально-педагогічної роботи).

Для правильного розуміння й тлумачення конфліктів, їхньої сутності, особливостей, функцій і наслідків важливе значення має типологізація, тобто вичленовування основних видів конфліктів на основі виявлення подібності та розходження, надійних способів ідентифікації конфліктів за спільністю істотних ознак і відмінностей.

Вид конфлікту - це варіант конфліктної взаємодії, який виділяється за певною ознакою. Залежно від кількості учасників конфлікти поділяють на внутрішньоособистісні, міжособистісні, групові, конфлікти між особистістю і групою.

Для вибору адекватного методу впливу й управління відповідним конфліктом доцільно проводити класифікацію залежно від основних ознак (табл. 3.1):

- способу розв’язання;
- сфери прояву;
- спрямованості впливу;
- ступеня виразності;
- кількості учасників;
- порушених потреб.

Таблиця 3.1

Класифікація конфліктів

Ознака класифікації	**Види конфліктів**
1. Спосіб розв’язання:	– насильницькі; – ненасильницькі
2. Сфера прояву:	– політичні; – соціальні; – економічні; – організаційні

Ознака класифікації	Види конфліктів
3. Спрямованість впливу:	– вертикальні; – горизонтальні
4. Ступінь виразності:	– відкриті; – приховані
5. Кількість учасників:	– внутріособистісні; – міжособистісні; – міжгрупові
6. Потреби:	– когнітивні; – конфлікти інтересів

1. Спосіб розв'язання конфліктів припускає їх розподіл на антагоністичні (насильницькі) конфлікти та компромісні (ненасильницькі).

Насильницькі (антагоністичні) конфлікти являють собою способи розв'язання суперечностей шляхом руйнування структур усіх сторін-конфліктерів чи відмови всіх сторін, крім однієї, від участі в конфлікті. Ця сторона і виграє. Наприклад: повна поразка супротивника в суперечці, вибори органів влади і т. д.

Компромісні конфлікти допускають декілька варіантів їх вирішення за рахунок взаємної зміни цілей учасників конфлікту, термінів, умов взаємодії.

Наприклад: постачальник не надсилає виробникові замовлену сировину в зазначений термін. Виробник має право вимагати виконання графіка постачань, але терміни поставок вантажу змінилися з причин відсутності засобів транспортування через неплатежі. За взаємної зацікавленості досягти компромісу можливо шляхом проведення переговорів, зміни графіка постачань.

3. Сфери прояву конфліктів вкрай різноманітні: політика, економіка, соціальні відносини, погляди й переконання людей.

Виділяють:

- політичні,
- соціальні,
- економічні,
- організаційні конфлікти.

Політичні конфлікти – зіткнення з приводу розподілу владних повноважень, форми боротьби за владу, політичної орієнтації, належності до конкретних політичних партій.

Соціальний конфлікт являє собою суперечності в системі стосунків людей (груп), що характеризується посиленням протилежних інтересів, тенденцій соціальних спільнот та індивідів. Різновидом соціальних конфліктів вважаються конфлікти трудові чи соціально-трудові, тобто у сфері трудової діяльності. Це велика група конфліктів, що останнім часом виникають у нашій країні дуже часто у вигляді страйків, пікетів, виступів великих груп працівників.

Економічні конфлікти являють собою широкий спектр конфліктів, в основі яких лежать суперечності між економічними інтересами окремих особистостей, груп. Це боротьба за певні ресурси, пільги, сфери економічного впливу, розподіл власності тощо. Зазначені види конфліктів поширені на різних рівнях управління. Економічні конфлікти являють собою широкий спектр конфліктів, що ґрунтуються на економічних інтересах окремих осіб, груп, організацій. Ці види конфліктів поширені на всіх рівнях управління. Наприклад, у 2002 р. економічні стосунки між Україною і США набули статусу конфліктного протистояння через те, що в нашій країні не було законодавства щодо регулювання випуску компакт-дисків.

Організаційні конфлікти є наслідком ієрархічних відносин, регламентування діяльності особи, застосування розподільчих відносин в організації: використання посадових інструкцій, функціонального закріплення за працівником прав та обов'язків; упровадження формальних структур управління; наявності положень з оплати й оцінювання праці, преміювання співробітників.

3. За спрямованістю впливу виділяють вертикальні й горизонтальні конфлікти. Характерною рисою їх є розподіл обсягу влади, який знаходиться в опонентів на момент початку конфліктних взаємодій.

У вертикальних конфліктах обсяг влади зменшується по вертикалі зверху донизу, що й визначає різні стартові умови для учасників конфлікту:

- начальник – підлеглий,
- вища організація – підприємство,
- засновник – мале підприємство.

У горизонтальних конфліктах відбувається взаємодія рівноцінних за обсягом наявної влади чи ієрархічним рівнем суб'єктів: керівники одного рівня, фахівці – між собою, постачальники – споживачі.

4. Ступінь виразності конфліктного протистояння припускає виділення прихованих і відкритих конфліктів.

Відкриті конфлікти характеризуються явно вираженим зіткненням опонентів: сварки, суперечки, зіткнення, військові протистояння.. Взаємодія регулюється нормами, що відповідають ситуації й статусу учасників конфлікту.

У разі прихованого конфлікту відсутні зовнішні агресивні дії між сторонами-конфліктерами, але при цьому використовуються непрямі способи впливу. Це відбувається за умови, що один з учасників конфліктної взаємодії побоюється іншого, або ж у нього немає достатньої влади й сил для відкритої боротьби.

5. Кількість учасників конфліктної взаємодії дозволяє поділяти їх на внутріособистісні, міжособистісні, міжгрупові.

Внутрішньоособистісні конфлікти являють собою зіткнення всередині особистості рівносильних, але протилежно спрямованих мотивів, потреб, інтересів. Особливістю даного виду конфлікту є вибір між бажаннями і можливостями, між необхідністю виконувати і дотриманням необхідних вимог. Прикладами є конфлікти "плюс - плюс", "плюс - мінус", "мінус - мінус". Конфлікти "плюс - плюс" передбачають вибір одного з двох сприятливих варіантів, наприклад: куди поїхати відпочивати або що придбати (автомобіль якої марки)? При цьому хоч вибір здійснюється з бажаних альтернатив, конфлікт може супроводжуватися стресовими ситуаціями, оскільки сам вибір часто буває складним і болісним. Конфлікти "плюс - мінус" - це конфлікти, за яких приймається рішення, коли кожний з варіантів містить і позитивні, і негативні наслідки, а вибрати потрібно один з урахуванням вирішення загального завдання. Наприклад, звільнення підлеглого є альтернативою для керівника:

а) позитивний аспект - звільнення неугодного працівника

б) негативний аспект - необхідність знайти нового співробітника.

У даному випадку приходиться прораховувати ряд варіантів та необхідні емоційні і матеріальні витрати для реалізації поставленого завдання.

Конфлікти "мінус - мінус" - це конфлікти, при яких у однієї особистості виникає необхідність приймати рішення, всі варіанти якого мають негативні наслідки. Наприклад, на вакантну посаду претендують дві кандидатури, які не

повністю відповідають кваліфікаційним вимогам. Керівник має зробити вибір, оскільки в даній ситуації він обмежений у часі.

Різновидом в*нутрішньоособистісних* конфліктів є рольові конфлікти, коли до однієї людини висуваються суперечливі вимоги щодо того, яким має бути результат її роботи. При цьому виникає необхідність одночасно виконати декілька особистих ролей (функцій). Наприклад: майстрові виробничої ділянки надіслано вказівку від начальника цеху нарощувати випуск продукції, а керівник служби якості наполягає на підвищенні якості продукції шляхом уповільнення виробничого процесу. Майстрові давалися суперечливі вказівки, причому одночасно. Даний конфлікт у результаті може бути зведено до конфлікту «мінус-мінус», оскільки майстра поставлено перед проблемою вибору: що робити, чию вказівку виконувати, за рахунок чого це робити.

Внутрішньоособистісний конфлікт може також виникнути тоді, коли виробничі вимоги не узгоджуються з особистими потребами або цінностями працівника. Наприклад, працівник планував у вихідні дні відпочити із сім'єю, але в п'ятницю керівник відділу поставив його перед фактом виробничої необхідності вийти на роботу у вихідні дні.

Внутрішньоособистісний конфлікт може також бути відповіддю на робоче перевантаження чи недовантаження. Такий конфлікт пов'язаний з низьким ступенем задоволеності роботою, малою впевненістю в собі і в організації, а також зі стресовими ситуаціями. Складність вирішення внутрішньоособистісних конфліктів полягає в тому, що іноді стикаються три складових, необхідних для досягнення поставленої мети: 1) бажання (хочу); 2) можливості (можу); 3) необхідність (треба). Наприклад:

- треба, але не хочу;
- хочу, але не можу;
- не хочу, але повинен.

Внутрішньоособистісний конфлікт може також виникнути в результаті того, що виробничі вимоги не збігаються з особистими потребами чи цінностями працівника.

Міжгрупові конфлікти – конфлікти між різними групами, підрозділами, у яких зачіпаються інтереси людей, об’єднаних на період конфлікту в єдині згуртовані спільноти. У міжгруповому конфлікті протиборчими сторонами виступають групи (малі, середні або мікрогрупи). В основі такого протиборства лежить зіткнення протилежно спрямованих групових мотивів (інтересів,

цінностей, цілей). У цьому полягає одна з особливостей цих конфліктів. Також слід зазначити, що ця згуртованість може зникнути відразу після припинення конфлікту, але в момент відстоювання загальних інтересів єдність групи може бути досить значною.

Міжособистісні конфлікти являють собою зіткнення індивідів із групою, між собою на підставі протилежно направлених мотивів, боротьбу за інтереси кожної зі сторін. Ці конфлікти найбільше розповсюджені, адже вони охоплюють практично всі сфери людських відносин. Будь-який конфлікт зводиться до міжособистісного. Навіть у міждержавних конфліктах трапляються зіткнення між лідерами або представниками держав. Саме цей тип конфліктів досить розповсюджений у виробничих колективах, сім'ї, суспільному середовищі. Наприклад, два дизайнери працюють над однією рекламою, але мають різні точки зору щодо способу її подачі. Аналогічним може бути конфлікт між двома кандидатами на підвищення при наявності однієї вакансії. Міжособистісний конфлікт може також проявлятися при прямому зіткненні особистостей. Люди з різними рисами характеру, поглядами і цінностями іноді просто не в змозі полагодити між собою. Як правило, погляди і цілі таких людей розрізняються докорінно. Міжособистісні конфлікти мають такі специфічні властивості:

- протиборство людей відбувається безпосередньо (суперники стикаються лицем до лиця);
- проявляється весь спектр об'єктивних і суб'єктивних причин;
- висока емоційність;
- зачіпаються інтереси не тільки суб'єктів конфлікту, а й тих, з ким вони безпосередньо пов'язані службовими або міжособистісними відносинами;
- міжособистісні конфлікти є своєрідним полігоном для перевірки характерів, темпераментів, інтелекту, волі та інших індивідуально-психологічних властивостей суб'єктів конфліктного протистояння.

6. Залежно від порушених потреб виділяють когнітивні конфлікти та конфлікти інтересів

Конфлікт когнітивний[55] – конфлікт поглядів, точок зору, знань. У такому конфлікті метою кожного суб’єкта є переконати опонента, довести правильність своєї точки зору, своєї позиції. Конфлікт когнітивний - це конфлікт поглядів з визначеної проблеми, тобто когнітивних структур. У такому конфлікті метою

[55] Когніти́вний - від лат. cognitio – пізнання, пізнавання, ознайомлення.

кожного суб'єкта є: переконати опонента; довести свою точку зору; боротися згідно з принципами власної або групової політики. Наприклад: численні дебати у Верховній Раді з виступами представників різноманітних фракцій; обговорення наукових та виробничих проблем на конференціях, зборах, нарадах. Відмінності між ідеологіями, культурами, релігіями не завжди зачіпають добрі відносини між опонентами. Якщо ж одна із сторін поставила за мету перемогти будь-якою ціною свого опонента і допускає застосування при цьому сили або інших засобів впливу, то в цьому випадку конфлікт може перетворитися у міжгруповий, соціальний.

Конфлікти інтересів можна представити як противагу конфлікту когнітивному, що означає протиборство, засноване на зіткненні інтересів різних опонентів (груп, індивідів, організацій).

У зв'язку з тим, що розподіл конфліктів на види представляється досить умовним, чіткої межі між різними видами не існує і на практиці виникають такі конфлікти:

- організаційні вертикальні міжособистісні;
- горизонтальні відкриті міжгрупові і т. д.

МЕЖІ КОНФЛІКТУ

Виділяють три аспекти визначення меж конфлікту:

1) просторовий;
2) часовий;
3) суб'єктний.

Просторові межі конфлікту - це визначення територій, на яких відбувається конфлікт. Чітке визначення просторових меж дуже важливе передусім для соціальних і міжнародних конфліктів. Знання меж конфлікту дає змогу вибрати адекватну форму впливу для його урегулювання.

Наприклад, у підрозділі організації виник конфлікт між керівником і підлеглим. Деякий час з'ясування стосунків не виходило за межі підрозділу. Оскільки конфлікт не припинявся, з плином часу інформація про нього поширилася на всю організацію, до конфлікту почали долучатися працівники інших підрозділів. Таке поширення конфлікту привело до необхідності приймати рішення на рівні керівництва організації, що, в свою чергу, позначилося на службовому становищі співробітника і керівника даного підрозділу.

Часові межі фіксують тривалість конфлікту у часі, його початок і кінець. Ці аспекти конфлікту впливають на юридичне оцінювання дій його учасників.

Наприклад, у кодексі законів про працю визначені положення щодо стягнень з порушників трудової дисципліни у відповідності з моментом оформлення відповідних матеріалів.

Суб'єктні межі конфлікту визначають кількість його учасників на початку. Розширення цієї межі, залучення до конфлікту нових осіб призводить до ускладнення структури конфлікту і пошуку інших способів його вирішення. Крім того розширення суб'єктних меж конфлікту може взагалі змінити характер його протікання. Наприклад, через затримку виплати заробітної плати організаційний конфлікт може перерости в страйк, вимагаючи зовсім інших підходів до його розв'язання.

Межі конфлікту нерозривно пов'язані з моментом його початку і закінченням конфліктного протистояння. *Початок конфлікту*, як правило, визначається об'єктивними (зовнішніми) ознаками, спрямованими проти іншого учасника. Якщо той усвідомлює, що ці акти спрямовані проти нього і їм протидіє, то конфлікт починається. Якщо дії не починаються, то має місце лише конфліктна ситуація. Це означає, що для визначення конфлікту, що вже почався, необхідно три умови:

- перший учасник свідомо і активно діє на шкоду своєму опоненту;
- опонент усвідомлює, що вказані дії спрямовані проти його інтересів;
- усі учасники приймають агресивні дії у відповідь.

Таким чином, конфлікт відсутній, якщо діє лише один учасник або учасники лише планують і обмірковують свої дії. Конфлікт починається тоді, коли сторони активно протистоять одна одній, переслідуючи свої цілі (до цього моменту ми маємо конфліктну ситуацію). Розвиток конфлікту, як правило, відбувається з поступовим розширенням складу його учасників, іноді і предмета конфлікту: виникнення невеликої конфліктної ситуації втягує у взаємодію двох суб'єктів, ті, в свою чергу, своїх захисників; зачіпаються інтереси свідків, розростається предмет конфлікту і склад його учасників. *Закінчення конфлікту* - це процес припинення дій усіх протиборчих сторін незалежно від причин початку конфлікту.

Конфліктологами розроблені і продовжують розроблятися засоби запобігання, профілактики конфліктів і методи їх "безболісного" розв'язання.В ідеалі вважається, що менеджер повинен не усувати конфлікт, а управляти ним і ефективно його використовувати (рис 3.3).

Рис. 3.3. Дії керівника при розв'язанні конфлікту

Перший крок в управлінні конфліктом полягає у розумінні його джерел. Менеджеру слід з'ясувати: це проста суперечка про ресурси, непорозуміння з якоїсь проблеми, різні підходи до системи цінностей людей або це конфлікт, що виник внаслідок взаємної нетерпимості (непереносимості), психологічної несумісності. Після визначення причин виникнення конфлікту, він повинен мінімізувати кількість його учасників. Встановлено, що чим менше осіб бере участь у конфлікті, тим менше зусиль потрібно для його розв'язання.

Існують три точки зору на конфлікт:

1) менеджер вважає, що конфлікт не потрібний і завдає тільки шкоду організації. І, оскільки конфлікт – це завжди погано, справа менеджера – усунути його будь-яким способом;

2) прихильники другого підходу вважають, що конфлікт – небажаний, але поширений побічний продукт організації. У цьому випадку вважається, що менеджер повинен усунути конфлікт, де б він не виникав;

3) менеджери, які дотримуються третьої точки зору, вважають, що конфлікт не тільки неминучий, але й необхідний і потенційно корисний. Наприклад, це може бути трудовий спір, в результаті якого народжується істина. Вони вважають, що як би не зростала і управлялася організація, конфлікти будуть виникати завжди, і це цілком нормальне явище.

Залежно від точки зору на конфлікт, якої дотримується менеджер, буде залежати процедура його подолання. У зв'язку з цим виділяють дві великі групи способів управління конфліктом: педагогічні й адміністративні (рис. 3.4).

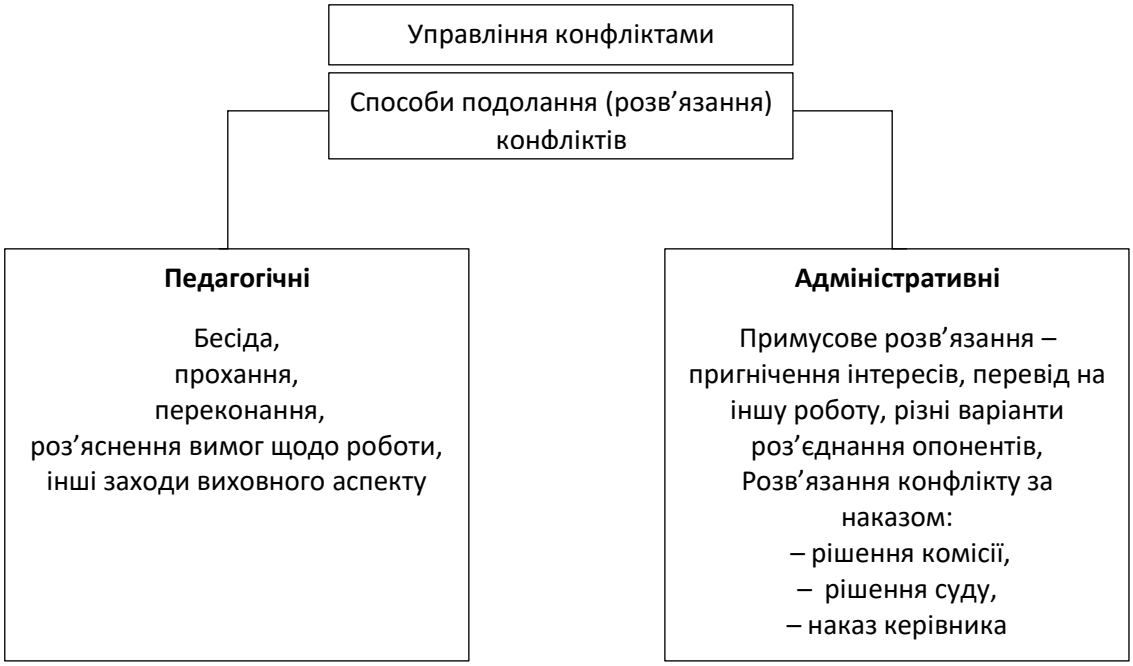


Рис. 3.4. Управління конфліктами

Поведінка менеджера в умовах конфлікту має по суті два незалежні виміри:

1) напористість, наполегливість – характеризує поведінку особистості, спрямовану на реалізацію власних інтересів, досягнення власних, часто меркантильних цілей;

2) кооперативність – характеризує поведінку, спрямовану на врахування інтересів інших осіб (особи) для того, щоб йти назустріч задоволенню їх (його) потреб.

Способи розвязання конфліктів.

У класичному менеджменті існує кілька ефективних способів управління конфліктною ситуацією. їх можна розділити на дві категорії: структурні і міжособистісні.

Структурні *методи вирішення конфліктів* – це методи впливу переважно на організаційні, трудові конфлікти, що виникли при неправильному розподілі повноважень, організації праці, прийнятої системи мотивації. До них відносять: роз'яснення вимог до роботи, використання координаційних і інтеграційних механізмів, встановлення комплексних цілей, використання системи винагород.

Роз'яснення вимог до роботи. Це один з кращих методів управління, що запобігає дисфункціональним конфліктам. Потрібно роз'яснити, які результати

очікуються від кожного співробітника і підрозділу. Тут повинні бути згадані такі параметри, як рівень досягнутих результатів, хто надає і хто отримує різну інформацію, система повноважень і відповідальності, а також чітко визначена політика, процедури і правила. Керівник усвідомлює ці питання не для себе, а доносить їх до підлеглих для того, щоб вони зрозуміли, чого від них очікують в тій або іншій ситуації.

Використання координаційних та інтеграційних механізмів. Один з найпоширеніших механізмів – ланцюг команд. Встановлення ієрархії повноважень упорядковує взаємодію людей, прийняття рішень і інформаційні потоки всередині організації. Якщо два або більше підлеглих мають розбіжності з якогось питання, конфлікту можна уникнути, звернувшись до загального керівника, пропонуючи йому прийняти рішення. Принцип єдиноначальності полегшує використання ієрархії для управління конфліктною ситуацією, бо підлеглий знає, чиї рішення він повинен виконувати.

Не менш корисні засоби інтеграції, такі як міжфункціональні групи, цільові групи, спільні наради відділів.

Встановлення комплексних цілей. Ефективне здійснення цих цілей вимагає спільних зусиль двох або більше співробітників або відділів, груп. Ідея, яка покладена в основу цієї методики – направити зусилля всіх учасників на досягнення спільної мети.

Використання системи винагород. Винагороди можна використовувати як метод управління конфліктом, здійснюючи вплив на людей, для запобігання дисфункціональних наслідків. Люди, які вносять свій внесок у досягнення комплексних цілей, допомагають іншим групам організації і намагаються підійти до вирішення проблеми комплексно, повинні винагороджуватися вдячністю, премією, визнанням чи підвищенням по службі. Не менш важливо, щоб система винагород не заохочувала неконструктивну поведінку окремих осіб і груп. Систематичне скоординоване використання системи винагород для заохочення тих, хто сприяє здійсненню загальної мети, допомагає людям зрозуміти, як їм слід поводитися в конфліктній ситуації.

Індивідуальна робота фахівця кібербезпеки сприяє тому, що в організації, яка займається захистом інформації, в основному виникають внутріособистісні та міжособистісні види конфліктів. Особливу складність для менеджера представляє знаходження способів розв'язання міжособистісних конфліктів. У цьому сенсі існує кілька можливих стратегій поведінки та відповідних варіантів

дій менеджера, спрямованих на ліквідацію конфлікту. Поєднання цих параметрів при різному ступені їх вираженості визначає п'ять основних способів розв'язання міжособистісних конфліктів.

Міжособистісні стилі вирішення конфліктів – це ухилення, згладжування, примус, компроміс і вирішення проблеми (співробітництво).

Ухилення. Цей стиль ґрунтується на тому, шо людина намагається уникнути конфлікту, ситуації, що провокує протиріччя й обговорення питання, який призводить до конфлікту.

Згладжування. Цей стиль характеризується поведінкою, яка продиктована переконанням, що не варто конфліктувати, тому що це негативно позначиться на всіх. Потрібно стимулювати почуття спільності між членами колективу.

Примус. У рамках цього стилю переважають намагання примусити прийняти свою точку зору будь-якою ціною, небажання цікавитися думкою інших. Особа при цьому веде себе агресивно і впливає на опонентів силою влади. Цей стиль ефективний, коли керівник має велику владу над підлеглими. Недоліком цього стилю є те, що присікається ініціатива підлеглих і не враховуються їх думки, інші важливі фактори, оскільки береться до уваги тільки одна точка зору.

Компроміс. Характеризується прийняттям точки зору іншої сторони, але лише до певної межі. Це дуже цінується в управлінських ситуаціях, тому що зводить до мінімуму недоброзичливість і дає можливість вирішити конфлікт, щоб задовольнити всі сторони. Але слід пам'ятати, що використання цього методу на ранній стадії розвитку конфлікту може зашкодити справі і його рішенню.

Рішення проблеми (співробітництво) – це визнання відмінностей в думках і готовність ознайомитися з іншими точками зору, щоб краще зрозуміти причину конфлікту і знайти вихід, прийнятний для всіх сторін. Той, хто використовує такий стиль, не прагне досягти своїх цілей за рахунок інших, а скоріше шукає найкращий варіант вирішення конфліктної ситуації.

В залежності від вибору способу розвязання буде отриманий результат, схема якого показана на рис. 3.5.

Рис. 3.5. Величина отриманого результату в залежності від способу розвязання конфлікту

Крім названих п'яти основних у їх рамках зустрічаються і інші прийоми розв'язання міжособистісних конфліктів:

1) координація – узгодження тактичних підцілей, поведінки в інтересах головної мети або рішення загальної задачі. Таке узгодження може проводитися між організаційними одиницями на різних рівнях управлінської піраміди (вертикальна координація); на організаційних рівнях одного рангу (горизонтальна координація) і у вигляді змішаної форми обох варіантів. Якщо узгодження вдається, то конфлікти вирішуються з меншими витратами і зусиллями;

2) інтегративне рішення проблеми. Дана техніка вирішення конфлікту ґрунтується на передумові того, що може існувати таке рішення проблеми, яке включає і усуває конфліктні елементи обох позицій, що прийнятно для обох сторін. Вважається, що це одна з найбільш успішних стратегій поведінки менеджера в конфлікті, тому що в цьому випадку вони найближче підходять до розв'язання проблем, які спочатку породили конфлікт. Однак підхід за принципом вирішення проблем часто важко втілюється в життя. Це пов'язано з тим, що він багато в чому залежить від професіоналізму і навичок в управлінській діяльності менеджера і, крім того, в цьому випадку для вирішення конфлікту потрібно багато часу. У цих умовах менеджер повинен мати хорошу технологію – модель для вирішення проблем;

3) конфронтація як шлях вирішення конфлікту. Мета конфронтації полягає в тому, щоб винести проблему на загальний розсуд. Це дає можливість вільно обговорювати її із залученням максимальної кількості учасників конфлікту (а по

суті – це не конфлікт, а трудовий спір), заохочувати вступ в конфронтацію з проблемою, а не один з одним з тим, щоб виявити і усунути перешкоди.

Мета конфронтаційних засідань – звести людей разом на неворожому форумі, який сприяє спілкуванню. Публічне і відверте спілкування є одним із засобів управління конфліктом.

Метод форсування. Примус до прийняття однієї точки зору. Цей стиль ефективний, коли керівник має велику владу над підлеглими.

Отже, у складних ситуаціях, де різноманітність підходів і точна інформація є запорукою для прийняття розумних рішень, появу конфліктних ситуацій потрібно навіть стимулювати, використовуючи її як один із засобів вирішення проблем. Однак при цьому необхідно володіти способами вирішення та виходу з конфліктних ситуацій.

Наприклад, конфлікт у кібербезпеці може виникнути між двома компаніями, які працюють у схожих галузях та конкурують між собою за клієнтів. Одна з компаній може намагатися зламати безпеку інформаційних систем своєї конкурентки, використовуючи для цього шкідливі програми, фішингові атаки або інші методи.

Розв'язання цього конфлікту може бути складним, оскільки потребує залучення експертів з кібербезпеки та визначення етичних принципів. Перш за все, необхідно провести детальний аналіз та зрозуміти, чи є фактичні докази порушення безпеки інформаційних систем. Якщо докази знайдені, можна звернутися до правоохоронних органів та вести судову боротьбу.

Однак, якщо доказів немає, можна спробувати залучити компанії до діалогу та переговорів. При цьому важливо дотримуватися принципу пропорційності та визначити етичні межі для розв'язання конфлікту. Можливим рішенням може бути залучення незалежного експерта з кібербезпеки, який допоможе визначити проблеми та запропонує шляхи їх вирішення.

Крім того, можна спробувати залучити сторони до співпраці у сфері кібербезпеки, щоб підвищити рівень безпеки даних та інформації у галузі в цілому. Наприклад, компанії можуть створити спільний комітет з кібербезпеки, який буде моніторити загрози та розробляти заходи забезпечення безпеки.

Після проведення розслідування виявилося, що ситуація виникла через недбале ставлення до захисту паролів і інших конфіденційних даних працівниками компанії. За рекомендаціями команди з інформаційної безпеки, було проведено навчання працівників з питань безпеки та прийнято нові

стандартні процедури в роботі з конфіденційною інформацією. Також були запроваджені системи моніторингу та контролю за доступом до конфіденційної інформації, що дозволить уникнути подібних ситуацій у майбутньому.

Найбільш ефективний спосіб запобігти внутрішньоособистісним і міжособистісним конфліктам, що можуть виникнути в підрозділі кібербезпеки, - організація превентивних заходів, які керівництво фірми (організації, установи) має виробити з самого початку при прийнятті на роботу [65]:

1) аналіз робочого місця (оцінювання наявних інформаційних, фінансових і людських ресурсів; складання портрета ідеального співробітника, характеристики якого повністю відповідають вимогам даного робочого місця; визначення майбутніх перспектив компанії та формування програми їх реалізації);

2) добір майбутніх співробітників за критеріями освіти, комунікабельності, досвіду, уміння ухвалювати рішення в екстремальних ситуаціях тощо;

3) проведення попередньої бесіди з добору кадрів та заповнення бланка заяви;

4) перевірка рекомендацій і зобов'язань перед іншими фірмами;

5) ухвалення остаточного рішення.

Висновок. Загалом, подібні конфлікти у кібербезпеці можуть виникати через недосконаліть технічних засобів захисту, людський фактор або через комбінацію обох факторів. Для їх вирішення необхідно проводити ретельний аналіз причин виникнення та розробляти цілеспрямовані заходи для запобігання подібних випадків у майбутньому. Важливо також розробляти плани дій у разі виявлення інцидентів в кібербезпеці та проводити навчання працівників з питань безпеки. Тільки комплексний підхід може гарантувати ефективний захист від потенційних загроз у кіберпросторі.

 *Питання для самоконтролю*:

1.В чому причина конфліктів?

2.Які види конфліктів є?

3.Які способи вирішення конфліктних ситуацій?

4.Які засоби запобігання, профілактики конфліктів і методи їх "безболісного" розв'язання?

Завдання:

1. Скласти анкету для заповнення претендентом на посаду в організації кібербезпеки з питаннями, що стосуються захисту інформації.
2. Скласти портрет ідеального працівника відділу інформаційної безпеки комерційного банку, використовуючи «Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України». URL: https://zakon.rada.gov.ua/laws/show/v0365500-11.

3.2. Методологічні засади конфліктології в кібербезпеці. Методи подолання конфліктів

Конфліктологія як окрема галузь наукових знань, виникла, розвивається й удосконалюється під впливом такого важливого чинника, як потреба суспільства в гармонізації відносин між окремими людьми, групами, об'єднаннями, державами та іншими структурними елементами, між якими можуть виникнути (й виникають) серйозні суперечності, розходження, конфлікти, війни тощо.

Методологічні основи конфліктології зорієнтовані на вивчення конфліктів і причин, що сприяють їх виникненню, на розкриття закономірностей цієї сфери суспільних явищ і процесів, на пошук шляхів розв'язання конфліктів. З метою наукового аналізу конфліктологія спирається на відомі закони і категорії філософської науки. Наприклад, закон єдності й боротьби протилежностей є методологічною основою вивчення особистості, в якій поєднуються позитивні та негативні риси, якості, а також розкриваються причини конкретного виду конфлікту.

Такі поняття, як необхідність і випадковість, причина й наслідок, загальне й одиничне, сутність і явище, сприяють розкриттю змісту однойменних понять у конфліктології. Це допомагає встановити причини конфліктів, їхні мотиви і до певної міри спрогнозувати індивідуальну конфліктну поведінку.

Які ж найуживаніші методи дослідження можна використати у процесі прогнозування й визначення проблемних ситуацій та конфліктів?

Найпоширенішими вважаються методи спостереження, системний, історичний, конкретно-соціологічних досліджень, аналізу документів, статистичний, біхевіористський, раціонально-інтуїтивний та ін.

В таблиці 3.2 наведений розподіл конкретних методів між групами дослідження.

Таблиця 3.2

Методи конфліктологічних досліджень

№п/п	Група методів	Конкретні методи
I	Методи вивчення та оцінки особистості	Спостереження, Опитування, Тестування
II	Методи вивчення та оцінки соціально-психологічних явищ у групах	Спостереження, Опитування, Соціометричний метод
III	Методи діагностики та аналізу конфлікту	Спостереження, Опитування, Аналіз результатів діяльності, Метод експертного інтерв'ю
IV	Методи керування конфліктами	Структурні методи Метод картографії

Розглянемо деякі з методів, що використовуються у конфліктології.

Системний метод. Системність вивчення будь-якої проблеми передбачає порівняно цілісне її вивчення, проте складність застосування системного підходу до вивчення конфліктів полягає зокрема в тому, що сам об'єкт дослідження не є системою в точному розумінні цього слова; нині методичний апарат ще не є самодостатнім.

Емпіричний[56] *підхід*. Для розв'язання конфліктів важливо забезпечити оптимальне співвідношення емпіричного і теоретичного компонентів пізнання при їх вивченні.

Ситуативний підхід. Передбачає вибір як одиниці аналізу конфліктної взаємодії конфліктної ситуації, що має певні часові та просторові межі, та ґрунтовний набір змістових характеристик конфлікту. Він є описовою, динамічною моделлю конфлікту. У міждержавному масштабі науковці

[56] Емпіричні дослідження – спостереження і дослідження конкретних явищ, експеримент, а також узагальнення, класифікація та опис результатів дослідження і експерименту, впровадження їх у практичну діяльність людей.

пропонують застосовувати для розгляду можливого варіанту стримування від агресії у конфлікті в інформаційному просторі розроблену модель на основі рефлексивної теорії ігор. У цій моделі запропоновано концепцію формалізації міждержавного інформаційного стримування на основі теорії рефлексивного управління В. Лефевра. На відміну від класичної теорії ігор, такий підхід враховує можливу ірраціональність поведінки людини (держави) у поєднанні з морально-мотиваційним та прагматичним аспектами вибору. Адекватність запропонованої моделі підтверджено аналізом прикладів інформаційного протиборства між Україною та Росією у пострадянський період [65, 66].

Статистичний метод. Сприяє вивченню багатьох випадків і дає змогу завдяки отриманим статистичним даним встановити закономірності, взаємозалежності, допомагає зробити узагальнення.

Метод експертних оцінок. Застосовується для прогнозування розвитку тих чи інших явищ. Конфліктологи використовують його для прогнозування конфліктів, оцінювання рівнів латентних конфліктів. Основою якісної та кількісної оцінки об'єктивних і суб'єктивних факторів, які впливають на конфлікт, стає думка спеціалістів, що спирається на їхній професійний науковий та практичний досвід. Важливо в цьому контексті сформулювати питання, правильно підібрати експертів, організувати їхню роботу.

Метод "картографії конфлікту". Суть методу полягає у послідовному заповненні "карти" конфлікту (рис. 3.6), розділеної на кілька секторів (залежно від кількості учасників конфлікту). У центр її заноситься основна проблема, а в розділи - інформація про учасників конфлікту та їхню мету в ньому.

Комп'ютерний контент-аналіз. Так званий комп'ютерний контент-аналіз (ККА) текстів засобів масової комунікації - один із методів відстежування моделей соціальної реальності, які транслюються масовими інформаційними та пропагандистськими джерелами. Ці результати можна використати як вихідну базу даних чи додатковий аналітичний матеріал у процесі прийняття рішень. Метод ККА досить швидко входить у сучасну практику.

Примирні та арбітражні процедури. Використовуються з метою розв'язання конфліктів на різних соціальних рівнях. Вони допомагають мирно врегульовувати складні трудові конфлікти, що зайшли в глухий кут. У такому разі аналіз конфліктів здійснюють незалежні організації. Наприклад, в Україні такою організацією є Національна служба посередництва і примирення (НСПП).

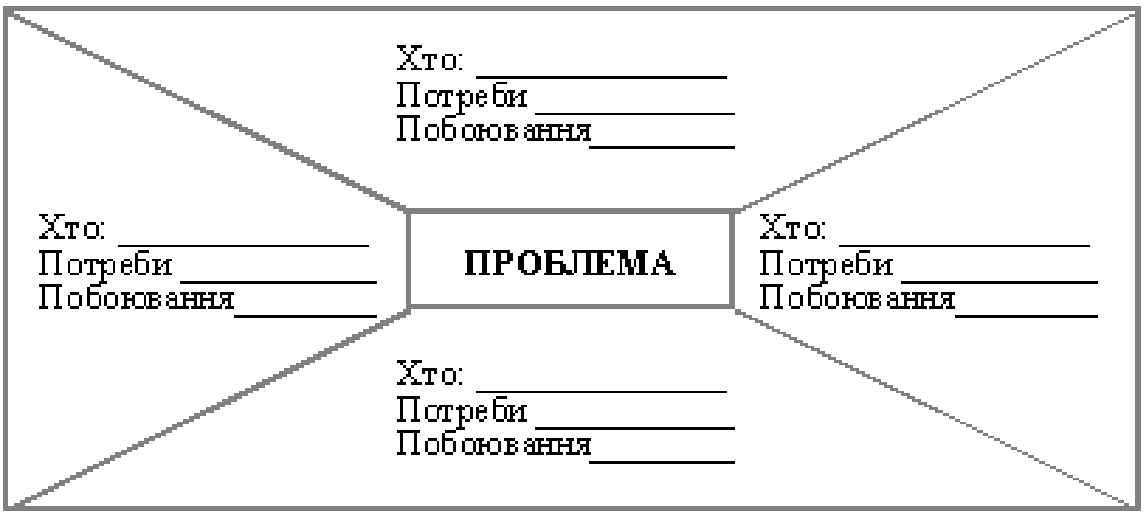


Рис. 3.6. Схема підготовленої карти конфлікту

Завданням незалежної організації є вивчення ситуації та запропонування проекту вирішення конфліктів. До компетенції НСПП належить:

- здійснення реєстрації висунутих працівниками вимог та колективних трудових спорів (конфліктів);
- аналіз вимог, виявлення та узагальнення причин колективних трудових спорів (конфліктів), підготовка пропозицій для їх усунення;
- підготовка посередників та арбітрів, які спеціалізуються на вирішенні колективних трудових спорів (конфліктів);
- формування списків арбітрів та посередників;
- перевірка, в разі необхідності, повноважень представників сторін колективного трудового спору (конфлікту);
- посередництво у вирішенні колективного трудового спору (конфлікту);
- залучення до участі в примирних процедурах народних депутатів України, представників державної влади, місцевого самоврядування.

Якщо ж сторони не доходять згоди, то незалежна організація виносить свій вердикт, обов'язковий для конфліктуючих сторін.

Соціометрія. Цей метод прийшов у вітчизняну науку із зарубіжної соціології та соціальної психології. Сам термін "соціометрія" походить від латинської ***socius*** (співучасник) і ***metrim*** (вимірювання).

Соціометричне вимірювання у конфліктології передбачає вивчення емоційно-психологічних зв'язків між людьми. На думку винахідника цього методу американського вченого Я.Л. Морено, соціометричний метод являє собою систему технічних засобів і процедур для аналізу соціально-емоційних зв'язків індивіда з членами тієї групи, де він живе і працює.

Соціальне макро-середовище (система суспільних відносин) є об'єктивною основою для виникнення тих та інших взаємин особистості з людьми в групі. Мікро-середовище посідає проміжне становище у відносинах особи й суспільства, воно ніколи не є пасивним, посилюючи або ж знижуючи вплив суспільства на особу.

За допомогою соціометричних досліджень можна отримати зріз динаміки внутрішніх взаємин у групі, дати конкретну кількісну оцінку внутрішньо-групових і між-групових процесів спілкування, виявити характер психологічних взаємин, наявність лідерства, угруповань, конфліктних ситуацій. Важливим позитивом цього методу є простота й швидкість процедури дослідження.

Конфліктологія в інформаційній та кібербезпеці

В інформаційному суспільстві, де все більша кількість людей має доступ до інтернету та залежить від його послуг, кібербезпека стає все важливішою. Кібератаки можуть стати причиною значних фінансових втрат, витоку конфіденційної інформації та пошкодження репутації компаній та організацій. Крім того, кібербезпека може бути порушена не лише зовнішніми загрозами, але й внутрішніми конфліктами та проблемами між співробітниками. У таких випадках важливо мати ефективні методи подолання конфліктів.

В інформаційній безпеці існують різні методи подолання конфліктів, зокрема, дипломатія, компроміс, узгодження та силові методи. Дипломатія полягає в тому, що сторони конфлікту взаємодіють між собою, щоб знайти спільний шлях вирішення проблеми. Компроміс означає, що сторони конфлікту погоджуються на часткових відступах від своїх позицій, щоб досягти домовленості. Узгодження полягає в тому, що сторони конфлікту знаходять спільне рішення, яке задовольняє всіх учасників. Силові методи використовуються, коли інші методи не дають результату, і полягають у використанні сили для вирішення конфлікту.

Кібербезпека є однією з найважливіших сфер сучасного світу, оскільки від неї залежить стійкість і безпека інформаційних технологій та інтернету. Однак, як і в будь-якій галузі, і у сфері кібербезпеки існують різного виду конфлікти, які можуть призвести до порушення безпеки інформації та привести до серйозних наслідків [67].

Види етичних конфліктів у кібербезпеці можуть виникати на різних рівнях технологічного процесу, включаючи розробку програмного забезпечення, використання комп'ютерних систем та мереж, збір та зберігання даних тощо. Деякі з найбільш поширених видів етичних конфліктів у кібербезпеці включають наступні [67]:

1. Конфлікти між конфіденційністю та доступністю. У кібербезпеці можуть виникати конфлікти між необхідністю захищати конфіденційну інформацію та забезпеченням доступності інформації для виконання бізнес-завдань або забезпеченням національної безпеки.
2. Конфлікти між приватністю та безпекою. У кібербезпеці можуть виникати конфлікти між необхідністю захищати особисту інформацію та забезпеченням безпеки мереж та комп'ютерних систем.
3. Конфлікти між правами власності та вільним доступом до інформації. У кібербезпеці можуть виникати конфлікти між правами власників програмного забезпечення та необхідністю забезпечення вільного доступу до інформації.
4. Конфлікти між законними та не законними діями. У кібербезпеці можуть виникати конфлікти між діями, які є законними за одних обставин, та діями, які є незаконними за інших обставин.
5. Конфлікти між професійними стандартами та вимогами клієнтів. У кібербезпеці можуть виникати конфлікти між професійними стандартами та вимогами клієнтів щодо функціональності та безпеки програмного забезпечення.
6. Конфлікти між економічними інтересами та етичними принципами. У кібербезпеці можуть виникати конфлікти між економічними інтересами компаній та етичними принципами, такими як захист конфіденційної інформації та особистої приватності.
7. Конфлікти між безпекою та свободою слова. У кібербезпеці можуть виникати конфлікти між необхідністю захисту від кібератак та свободою висловлювання в Інтернеті.

8. Конфлікти між національною безпекою та глобальною свободою в Інтернеті. У кібербезпеці можуть виникати конфлікти між необхідністю захисту національної безпеки та глобальною свободою в Інтернеті.

Ці етичні конфлікти можуть бути дуже складними та заплутаними, і вирішення їх може вимагати компромісів між різними сторонами. Для успішного вирішення цих конфліктів важливо мати етичний фреймворк та професійну етику у кібербезпеці, які допоможуть знайти баланс між різними етичними принципами та вимогами.

Конфлікти в кібербезпеці становлять серйозну загрозу для безпеки та стабільності в кіберпросторі, тому важливо постійно працювати над їх протидією та розвитком заходів для запобігання новим загрозам. Це потребує співпраці та координації зусиль різних держав, організацій та суб'єктів кіберпростору, а також використання інноваційних методів та технологій.

Кібербезпека занадто довго вважалася третинним питанням для міжнародної безпеки. Це змінилося. Оскільки цифрові інфраструктури стають центральними в економічній та соціальній діяльності, здатність втручатися в них може мати серйозні негативні наслідки. Необхідність запобігання таким наслідкам стала центральним питанням національної та міжнародної безпеки. Важливість кібербезпеки для міжнародної безпеки буде продовжувати зростати, і порядок денний організації і форумів міжнародної безпеки повинен це відображати.

Сьогодні робота з кіберконфліктами, як питанням політики, знаходиться на ранній стадії, з деякими ранніми угодами, пов'язаними з імплементацією існуючого міжнародного права в кіберпростір, а також проектами норм і заходів зміцнення довіри.

Основною характеристикою кіберконфлікту є атрибуція атаки навіть окремими користувачами, не кажучи вже про спонсорство будь-якою державою, яка здатна працювати через ряд проксі-шарів (включаючи ботнети). Однак ще одною відмінністю між традиційною війною та можливою кібервійною є масштаб: кіберінциденти не відбуваються між двома країнами, тоді як інші країни мовчки спостерігають. Інтернет є глобальним ресурсом, і кіберзброя, така як ботнети, буде використовувати обчислювальні ресурси інших країн, роблячи кібервійну глобальною. Тому необхідно розуміти, що питання кіберконфліктів та кібервійськ належать до сфери управління Інтернетом і повинні обговорюватися разом з іншими загрозами безпеці.

Міжнародна увага до кібербезпеки різко зросла в останні роки, оскільки кіберпростір став центральною глобальною інфраструктурою. Це сприяє розвитку та зростанню, але також розширюєення можливості для конфліктів та злочинності. Держави визнали важливість кіберпростору, а разом з ним і необхідність глобального співробітництва, щоб зробити його більш стабільним і безпечним. Три групи GGE під проникливим керівництвом представників з Австралії Бразилії та Росії, змогли створити структуру для міжнародного обговорення безпеки та стабільності в кіберпросторі і, зрештою, основу для відповідальної поведінки держави. Основні елементи були викладені у звіті GGE[57] за 2010 рік. Вони є: (a) нормами, правилами і принципами відповідальної поведінки держави; (b) заходами зміцнення довіри; (c) заходами нарощування кіберпотенціалу. Ці елементи продовжують формувати міжнародну дискусію про кібербезпеку.

Кульмінація цих зусиль була в 2015 році, коли в Звіті GGE (Звіт групи урядових експертів про події у сфері інформації та телекомунікацій у контексті міжнародної безпеки (A/70/174)) було запропоновано 11 норм і заходів щодо поліпшення кібербезпеки. Ці норми встановлюють рамки відповідальної поведінки держави. На засіданні Генеральної Асамблеї 2015 року всі держави-члени ООН погодилися консенсусом керуватися цим Звітом 2015 року.

Звіти GGE міцно помістили державну практику кібербезпеки в існуючу структуру міжнародних відносин і міжнародного права. У цих доповідях рекомендувалося, щоб принципи суверенітету, рівності держав, Статут ООН і міжнародне право керували відносинами держав у кіберпросторі. Звіти включали рекомендації співпрацювати з іншими державами та допомагати їм, уникати дестабілізуючих дій (таких як використання проксі або незаконні атаки на критичну інфраструктуру), обмінюватися інформацією про загрози, конфлікти і вразливості в кіберпросторі та пом'якшення вразливостей, а також нарощувати кіберпотенціал.

Звіт за 2015 рік ґрунтувався на висновках Звіту за 2013 рік і закликав держави обмінюватися інформацією, співпрацювати у захисті критичної інфраструктури та допомагати один одному у переслідуванні кіберзлочинності. Звіт 2015 року підтвердив необхідність демонстрації повної поваги до прав

[57] "Звіт GGE" (англ. "The GGE Report") - це документ, який створюється робочою групою Генеральної Асамблеї ООН з питань інформаційно-комунікаційних технологій у контексті міжнародної безпеки (англ. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", скорочено GGE).

людини та приватного життя. Він рекомендував державам вжити заходів для забезпечення цілісності ланцюга поставок інформаційно-комунікаційних технологій, обмінюватися інформацією про вразливості інформаційної безпеки і не втручатися в роботу груп реагування на комп'ютерні надзвичайні ситуації інших країн.

Одним з найважливіших внесків Звіту за 2015 рік є рекомендація про те, що держава повинна захищати свою національну інфраструктуру і не повинна свідомо проводити або підтримувати дії, які навмисно завдають шкоди або погіршують критичну інфраструктуру, що суперечить її зобов'язанням за міжнародним правом. Це не заборона на кібератаки. Вони все ще дозволяються, якщо держави дотримуються загальних принципів «гуманності, необхідності, пропорційності та відмінності», визнаних у Звіті за 2015 рік.

Норми, узгоджені в GGE 2013 і 2015 років, є «необов'язковими». Держави не готові брати на себе офіційні, обов'язкові для виконання зобов'язання (наприклад, договір або конвенцію). Між націями існують розбіжності, які необхідно опрацювати в першу чергу. Зобов'язуючий договір зіткнеться з серйозними проблемами розробки узгоджених визначень, забезпечення відповідності та встановлення верифікації. Залишаються без відповідей питання щодо того, яка угода була б найбільш ефективною та складною проблемою визначення. Спроби визначити «інформаційну зброю», наприклад, швидко призводять до того, що переважна більшість комерційного використання та доступність інформаційних технологій не застосовується. Однак необов'язковість не означає, що узгоджені норми не мають ефекту.

Все це позитивні кроки, але в міжнародному співтоваристві залишається глибоке відчуття занепокоєння та занепокоєння щодо потенційної можливості зловмисних дій держави у кіберпросторі.

Джерелами цього занепокоєння є складність оцінки ризиків, створених новими технологіями та глибокими змінами в міжнародній системі, включаючи зростання нових впливових суб'єктів, тиск на міжнародні структури, створені в 1945 році, та зростання напруженості між великими державами. Кіберінциденти жвавішають в період зростаючих міждержавних конфліктів в цифровій сфері і міжнародні установи, створені після Другої світової війни, зазнають все більшого впливу на інформаційну інфраструктуру. У світлі цього виникає запитання, чи достатньо рамок 2015 року?

Вимірювання ефективності узгоджених норм і СБМ вимагає оцінки того, чи змінилася і як змінилася поведінка держави. Враховуючи ступінь прихованості, яка використовується в більшості кібероперацій, це важко розрахувати. Однак ряд країн дійшли висновку, що були випадки, коли норми не дотримувалися, і якщо наслідків за недотримання норм не було виявлено - стимули до зміни поведінки цих країн залишились невеликі. Висновок про те, що при порушенні норми повинні бути наслідки, переосмислить обговорення кібербезпеки.

Аналіз стану кіберзахисту країн останнім часом свідчить, що основним методом подолання конфлікту міжнародного масштабу є створення груп, комісій для обговорення на світовому рівні шляхів подолання, прийняття резолюцій, укладання та затвердження договорів або конвенцій та взяття зобов'язань виконувати домовленості.

Конфлікти в кібербезпеці не обмежуються рівнем міжнародних відносин.

Підприємствам, організаціям, які займаються захистом інформації та кібербезпекою, притаманні внутрішні та зовнішні конфлікти в цих організаціях. Їх загальна класифікація розглянуті в п. 3.1 цього посібника.

Одним з найпоширеніших видів конфліктів у кібербезпеці є атаки з боку зловмисників, які намагаються зламати систему захисту та отримати незаконний доступ до інформації. Ці атаки можуть бути здійснені за допомогою вірусів, троянських програм, фішингу, DDoS-атак, та інших методів. Щоб запобігти цим атакам, необхідно регулярно оновлювати програмне забезпечення, створювати складні паролі та користуватися двофакторною автентифікацією. Крім того, рекомендується використовувати антивірусне програмне забезпечення та встановлювати файрвол.

Інший вид конфлікту - це конфлікти в середині компанії. Ці конфлікти можуть виникати між різними підрозділами компанії, між співробітниками, а також між керівництвом та підлеглими. Щоб уникнути цих конфліктів, необхідно забезпечити правильну організацію внутрішньої структури компанії та забезпечити взаємодію між підрозділами та співробітниками. Для цього можна використовувати комунікаційні інструменти та платформи, проводити тренінги та семінари з кібербезпеки для всіх працівників компанії.

Крім того, у кібербезпеці можуть виникати конфлікти між компаніями або організаціями. Наприклад, можуть виникати спори щодо права власності на певні технології чи програмне забезпечення, зловживання під час конкуренції,

або порушення авторських прав. Для запобігання таких конфліктів необхідно ретельно дотримуватися законодавства та міжнародних стандартів щодо кібербезпеки, проводити перевірки безпеки, а також брати участь в консультаціях та переговорах для врегулювання спорів, використовуючи методи які були розглянуті у попередньому пункті.

Окрім зазначених видів конфліктів, у кібербезпеці можуть виникати й інші складні ситуації, які потребують вчасного та ретельного аналізу. Для подолання таких конфліктів необхідно використовувати спеціальні технології та методи, такі як кібераналітика, кіберсоціологія, кібердипломатія та інші.

Кібераналітика – комплексний аналіз інформації щодо кібербезпеки з метою виявлення потенційних загроз та вразливостей. Кібераналітика дозволяє швидко виявляти та вирішувати проблеми безпеки, визначати тенденції та прогнозувати можливі загрози.

Іншим методом є *кіберсоціологія* – вивчення поведінки користувачів в інформаційному просторі з метою виявлення потенційних загроз та ризиків. Кіберсоціологія дозволяє зрозуміти, які фактори впливають на поведінку користувачів та які заходи потрібно вжити, щоб зменшити ризики порушення кібербезпеки.

Також важливо використовувати *кібердипломатію* – комплекс заходів з міжнародної співпраці з метою забезпечення кібербезпеки. Відсутність або недосконалість стандартів та правил поведінки в кіберпросторі є однією з головних причин виникнення конфліктів в кібербезпеці. Кібердипломатія дозволяє вирішувати міжнародні конфлікти щодо кібербезпеки, створювати спільні стандарти та правила поведінки в кіберпросторі. Зокрема, Міжнародний союз з телекомунікацій ITU[58] (ITU - International Telecommunication Union) пропонує ряд стандартів та рекомендацій, що стосуються кібербезпеки. Наприклад, стандарт ITU-T X.1500 "Цілісність, конфіденційність та доступність інформації – загальні поняття та моделі" описує загальні поняття та моделі кібербезпеки, що допомагають забезпечити цілісність, конфіденційність та доступність інформації.

Для подолання конфліктів в кібербезпеці також важливо співпрацювати з правоохоронними органами та вести активну роботу з протидії кіберзлочинності.

[58] ITU - International Telecommunication Union - міжурядова організація, створена в 1865 році, сьогодні ITU є спеціалізованою організацією ООН, яка працює в галузі зв'язку та інформаційних технологій. Головне завдання ITU полягає у забезпеченні розвитку ефективних та доступних телекомунікаційних інфраструктур та послуг, сприянні глобальній координації використання радіочастот та супутникових орбіт, а також регулюванні телекомунікаційного ринку.

Наприклад, Міжнародний центр боротьби з кіберзлочинністю (IC3[59]) створений для збору та аналізу інформації про кіберзлочинність, а також для забезпечення співпраці між правоохоронними органами різних країн.

Для ефективної боротьби з конфліктами в кібербезпеці необхідно забезпечити постійне навчання та підвищення кваліфікації спеціалістів з кібербезпеки. Також важливо розробляти і впроваджувати нові методи та технології кібераналітики, кіберсоціології та кібердипломатії, необхідно створювати нові методи та інструменти для виявлення та протидії кіберзлочинності. Для цього потрібно використовувати інструменти машинного навчання, інтелектуальну аналітику даних та інші інноваційні технології з урахуванням етичних методів та інструментів, які дозволять досягти мирного та стійкого вирішення конфлікту.

Дипломатія, як найбільш етичний метод, може бути ефективним методом подолання конфлікту в кібербезпеці. Зокрема, важливо сприяти взаєморозумінню між сторонами конфлікту та створити підґрунтя для спільного пошуку рішень. Крім того, важливо визнавати права та інтереси інших сторін, щоб забезпечити баланс між потребами у безпеці та іншими аспектами, наприклад, свободою слова або приватністю.

Компроміс також може бути ефективним методом подолання конфлікту в кібербезпеці. Сторони конфлікту можуть знайти рішення, яке дозволить зменшити шкоду, спричинену конфліктом, та задовольнити потреби обох сторін. Наприклад, компанії можуть згодитись на спільний аудит системи безпеки, щоб забезпечити безпеку даних та зменшити ризик інформаційного витоку.

Узгодження є іншим ефективним методом подолання конфлікту в кібербезпеці. Сторони конфлікту можуть працювати разом, щоб знайти рішення, яке задовольняє всіх учасників та забезпечує безпеку даних та інформації. Наприклад, компанії можуть співпрацювати, щоб розробити стандарти безпеки та обмінюватись інформацією про потенційні загрози.

Силові методи, такі як судові процеси, можуть бути використані, коли інші методи не дають результату. Однак, використання силових методів може

[59] Міжнародний центр боротьби з кіберзлочинністю (англ. International Cybercrime Investigation Center, скорочено IC3) - це спільний проект Федерального бюро розслідувань (ФБР) та Національного центру інформаційної безпеки та захисту інфраструктури США (NCCIC), призначений для боротьби з кіберзлочинністю на міжнародному рівні.

спричинити додаткові конфлікти та погіршити стосунки між сторонами конфлікту.

Окрім того, важливо не забувати про захист основних прав та свобод людини в кіберпросторі. Це означає, що необхідно розробляти та впроваджувати механізми захисту персональних даних, приватності та свободи виразу, а також боротися з дезінформацією та впливом на масову свідомість в кіберпросторі.

Підсумовуючи, можна константувати такі методи не тільки подолання а й попередження конфліктів у кібербезпеці:

1. Міжнародна співпраця та створення правової бази. На міжнародному рівні важливо розвивати міждержавну співпрацю у сфері кібербезпеки та створювати міжнародні стандарти та правила. За допомогою такої співпраці можна розвивати єдиний підхід до протидії кіберзлочинності та створювати механізми обміну інформацією та координації дій у випадку кібератак.

2. Розробка та використання нових технологій. Одним із методів протидії кіберзлочинності є використання новітніх технологій. Наприклад, застосування штучного інтелекту для виявлення та аналізу кібератак, розробка блокчейн-технологій для забезпечення безпеки в Інтернеті речей та інше.

3. Підвищення кваліфікації фахівців з кібербезпеки. У сфері кібербезпеки важливо мати кваліфікованих фахівців з високим рівнем компетентності. Тому необхідно проводити навчання та підвищення кваліфікації спеціалістів з кібербезпеки, а також стимулювати розвиток цієї сфери.

4. Створення механізмів захисту основних прав та свобод людини в кіберпросторі. Для захисту основних прав та свобод людини в кіберпросторі необхідно розробляти та впроваджувати механізми захисту персональних даних, приватності та свободи виразу, а також боротися з дезінформацією та впливом в мережі.

5. Створення системи відповідальності за кіберзлочини. Для забезпечення ефективної боротьби з кіберзлочинами необхідно створити систему відповідальності за такі дії. Це може бути досягнуто шляхом введення строгих законів та накладання відповідних санкцій на кіберзлочинців.

6. Забезпечення відповідної технічної та фінансової бази для боротьби з кіберзлочинністю. Для ефективної боротьби з кіберзлочинами необхідно мати відповідну технічну та фінансову базу. Це може включати розробку нових технологій, вдосконалення наявних засобів захисту, підвищення якості мережі та обладнання та інше.

Отже, кібербезпека є важливою галуззю, в якій можуть виникати різноманітні конфлікти. Щоб запобігти цим конфліктам та забезпечити безпеку інформаційних технологій, необхідно використовувати різні методи та технології, зокрема оновлення програмного забезпечення, використання інноваційних технологій та методів кібераналітики, кіберсоціології та кібердипломатії, встановлення антивірусного програмного забезпечення та файрволів, правильну організацію робочого місця та вчасну реакцію на потенційні загрози. Крім того, важливо забезпечувати постійне навчання та підвищення кваліфікації спеціалістів з кібербезпеки.

Узагальнюючи, можна сказати, що конфлікти в кібербезпеці є невід' ємною складовою кібербезпеки в цілому, і виникнення нових загроз і методів нападу вимагає постійної адаптації та розвитку заходів для їх протидії. Серед видів конфліктів в кібербезпеці можна виділити конфлікти між державами, корпораціями, кіберзлочинцями та іншими суб'єктами кіберпростору. При цьому, застосування етичних норм забезпечить ефективне вирішення конфліктів.

Висновок. Кібербезпека є важливим аспектом сучасного світу, який вимагає постійного удосконалення та вдосконалення заходів безпеки. Однак, на шляху до досягнення цілей забезпечення безпеки даних та інформації, можуть виникати конфлікти, які можуть затримати розвиток у цій галузі. Методи подолання конфліктів у кібербезпеці, такі як дипломатія, компроміс, узгодження та силові методи, можуть допомогти сторонам знайти ефективні способи вирішення проблем та забезпечити безпеку даних та інформації.

Проте, важливо пам'ятати, що при вирішенні конфліктів у кібербезпеці потрібно керуватися етичними принципами. При вирішенні проблеми безпеки даних та інформації, необхідно враховувати права та інтереси інших сторін, дотримуватися принципу пропорційності та уникати неприпустимих методів та засобів.

Також, при вирішенні конфліктів у кібербезпеці важливо залучати всіх зацікавлених сторін, в тому числі експертів з кібербезпеки, щоб забезпечити якість та ефективність вирішення проблем та досягнення балансу між безпекою та іншими аспектами, що важливі для суспільства.

Питання для самоконтролю:

1.Які найуживаніші методи дослідження можна використати у процесі прогнозування й визначення проблемних ситуацій та конфліктів?

2.На що зорієнтована методологія конфліктів?

3.Які є шляхи подолання міжнародних конфліктів в кібербезпеці?

4.Які смислові методи подолання конфліктів можна застосувати у кібербезпеці?

Завдання:

1.Описати кіберпотенціал держави, підприємства, банку.

2.Навести приклад конфлікту з причини незадовільної комунікації та спланувати шляхи його розв’язання.

3.Визначити причину і спосіб вирішення конфліктів:

- урядова організація використовує програмне забезпечення для збору даних про користувачів Інтернету з метою запобігання кіберзлочинності, включаючи терористичні акти;
- компанія може хотіти зберігати особисту інформацію своїх клієнтів, щоб використовувати її для маркетингових цілей.

Розділ 4
МЕТОДИ ПРИЙНЯТТЯ ЕТИЧНИХ РІШЕНЬ В ПРОФЕСІЙНИХ СИТУАЦІЯХ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

4.1. Потенційні моральні проблеми в організації інформаційної безпеки корпорацій

У сучасному світі інформаційна безпека корпорацій є однією з найбільш важливих проблем. Зростаючі загрози з боку кіберзлочинців, зловживання працівниками доступом до конфіденційної інформації та інші виклики роблять інформаційну безпеку надзвичайно складною. Як і в будь-якій галузі, в організації інформаційної безпеки корпорацій існують потенційні моральні проблеми, які потрібно враховувати при розробці та впровадженні політик та процедур. Створення ефективної системи управління інформаційною безпекою є неможливим без чіткого визначення загроз інформації, що охороняється та супуніх їм проблем моралі.

Під загрозами інформації прийнято розуміти потенційні або реально можливі дії стосовно інформаційних ресурсів, що призводять до неправомірного володіння інформацією. Загроза інформаційної безпеки – це сукупність умов і факторів, що створюють небезпеку порушення інформаційної безпеки. В теорії конфліктології це називається створення конфліктної ситуації. Під загрозою (в загальному) також розуміється потенційно можлива подія, дія (вплив), процес або явище, які можуть призвести до заподіяння шкоди чиїм-небудь інтересам.

Ззагрозами інтересів суб'єктів інформаційних відносин є потенційно можливі події, процес або явище, які з допомогою впливу на інформацію або інші компоненти інформаційної системи, можуть прямо або опосередковано призвести до заподіяння шкоди інформаційним даним того чи іншого суб'єкта

До внутрішніх загроз інформаційної безпект відносять дії чи бездіяльність (навмисні чи не навмисні) співробітників, що протидіють інтересам діяльності підприємства, наслідком яких може бути нанесення економічних збитків компанії, втрата інформаційних ресурсів, підрив ділового іміджу компанії, виникнення проблем у відносинах з реальними чи потенційними партнерами тощо.

Причинами таких внутрішніх загроз (конфліктних ситуацій) можуть бути:

- непрофесійні дії працівників;
- *низький стан виховної та профілактичної роботи в організації*;
- недосконала система заробітної плати та стимулювання праці персоналу;
- порушення правил кадрової роботи, невідповідність кадрової політики умовам роботи в організації;
- *психологічні та комунікаційні особливості працівників*;
- відсутність нормативної бази організації, яка б установлювала режими їх діяльності та правила поведінки персоналу;
- *низький рівень стану трудової та виробничої дисципліни, слабка вимогливість керівного складу*.

У 1930-х і 1940-х роках обсяги доступних даних були мініскульптурними для порівняння, і «обробка» цих даних була повністю ручною. Якби існувала навіть невелика частина сьогоднішніх можливостей, світ, яким ми його тепер знаємо, напевно, був би зовсім іншим.

Технологічні досягнення як в апаратному, так і в програмному забезпеченні значно змінили сферу того, що можна накопичити і обробити. Величезна кількість даних, виміряних в петабайтах і більше, може бути централізовано збережена і отримана без зусиль і швидко з багатьох розрізнених джерел та за результатами синтезу може складати набір з новими значеннями, які в іншому контексті не можуть відповідати етичним нормам та створювати моральну проблему.

У цифрову епоху порушення даних, особливо використання персональних даних працівників компанії та повязані ними моральні проблеми є постійною потенційною проблемою для менеджерів корпорацій (компаній).

Уряди збирають величезні обсяги даних про фізичних осіб та організації та використовують їх для різних цілей: національної безпеки, точного збору податків, демографії, міжнародного геополітичного стратегічного аналізу тощо. Корпорації роблять те ж саме з комерційних причин; для збільшення бізнесу, контролю витрат, підвищення прибутковості, завоювання частки ринку і т.д. Інформація про працівників може бути зібрана та використана для забезпечення безпеки компанії або підвищення ефективності своєї управлінської діяльності, для перевірки нових працівників або виявлення інших потенційних загроз. Проте, при цьому можуть порушуватися приватність та особисті права

працівників. Крім того, збирання та використання даних можуть призвести до дискримінації за релігійними, расовими або іншими ознаками. Така інформація, як компенсаційні та довідкові дані, а також особиста ідентифікаційна інформація, номер соціального страхування та ідентифікатори облікового запису, повинна надійно зберігатися та доступ до неї має бути організований тільки уповноваженим персоналом. Системи, які відстежують ці дані, можуть бути захищені, але в якийсь момент дані при обміні інформацією повинні покинути ці системи і бути використані при передачі в установленому порядку. Операційна політика та процедури повинні упорядковувати належне поводження з цими даними, але якщо вони не дотримуються або не виконуються, навряд чи є сенс їх мати.

Іншою моральною проблемою є використання інформації в маніпулятивних цілях. Корпорації можуть використовувати дані про своїх співробітників та клієнтів для рекламних та маркетингових цілей, або для впливу на їхні поведінкові звички та відношення до певних продуктів чи послуг. Це може порушувати особисту свободу та незалежність людей, а також створювати несправедливі переваги для певних компаній на ринку.

Інша потенційна моральна проблема пов'язана з відповідальністю за безпеку даних. Компанії, в переважній більшості, мають інтерес зберігати конфіденційну інформацію про своїх клієнтів та працівників. Проте, зберігання цієї інформації повинно здійснюватися з відповідною дбайливістю та відповідним рівнем захисту. Якщо компанія не забезпечує належний захист даних то інформація може стати доступною кіберзлочинцям, що може привести до серйозних наслідків для компанії та її клієнтів. Отже, потрібно враховувати моральну відповідальність компанії за зберігання та захист даних.

Також, потенційним моральним питанням є використання програмного забезпечення для моніторингу працівників. Наприклад, компанії можуть встановлювати програмне забезпечення, щоб відслідковувати, як працівники використовують комп'ютери та Інтернет під час роботи. Це може бути важливим для забезпечення безпеки компанії але це також може порушувати приватність та особисті права працівників. Крім того, використання програмного забезпечення для моніторингу може підірвати довіру та взаємовідносини між компанією та її працівниками і буде причиною міжособистісного конфлікту.

Нарешті, іншим потенційним моральним питанням є те, що компанії можуть використовувати інформаційну безпеку як виправдання для обмеження

свободи слова та прав на доступ до інформації. Компанії можуть бути зацікавлені у запобіганні поширенню конфіденційної інформації або запобіганні витоку даних, але при цьому можуть обмежувати свободу думки та вільний доступ до інформації. Це може мати негативний вплив на відносини між компанією та її співробітниками, а також вплинути на довіру до компанії від зовнішніх зацікавлених сторін.

Ще одна потенційна моральна проблема пов'язана з використанням штучного інтелекту та автоматизованих систем для контролю та захисту інформації. Штучний інтелект може бути корисним для розпізнавання загроз та захисту від кібератак, але його використання може порушувати права та свободи людей. Наприклад, якщо компанія використовує автоматизовану систему моніторингу співробітників, то це може порушувати їх приватність та свободу.

Наразі компаніям і керівникам доступно дуже мало вказівок щодо того, як зменшити ризики витоку даних через зловмисних або недбалих інсайдерів[60].

Проведено багато досліджень [46, 48, 53, 62-67], в яких визначені фактори, що впливають на наміри співробітників порушити політику безпеки інформаційних систем організації, використовуючи гіпотетичні сценарії. Зокрема, у дослідженні [68] дані були зібрані від 173 студентів за допомогою інструменту онлайн-опитування та проаналізовані за допомогою множинної регресії. Дослідження має кілька практичних і теоретичних наслідків. Виявлена роль статі у зв’язку між моральними переконаннями, зрозумілістю політики безпеки, моральним питанням, що лежать в основі, і намірами порушити політику безпеки. Результати дослідження свідчать про те, що моральні переконання та розуміння політики безпеки знижують наміри порушити політику, і роблять це по-різному залежно від статі людини та основного морального питання. Отримані результати свідчать про те, що використання етичних і гендерних аспектів забезпечує додаткове розуміння питань інформаційної безпеки з урахуванням моральних цінностей. Отримані результати можуть допомогти менеджерам із інформаційної безпеки у розробці ефективної політики безпеки та розробці більш ефективних навчальних програм для фахівців кібербезпеки.

Широко поширена думка, що інсайдери всередині організації можуть бути більш небезпечними, ніж ті, хто знаходиться поза організацією, через їх глибоке

[60] Інса́йдер (англ. inside – укр. всередині) – це: будь-яка особа (юридична чи фізична), яка має доступ до конфіденційної інформації про діяльність фірми в силу свого службового становища або родинних зв'язків.

знання системи та привілей доступу [69]. Такі дії агентів-людей, як саботаж, можуть бути навмисними або ненавмисними чи випадковими, як, наприклад, забування змінити паролі. Тому загроза з боку інсайдерів незмінно зростає, коли співробітники не дотримуються політики та процедур інформаційної безпеки організації.

У літературі про інформаційні системи порушення політики безпеки розглядалися з багатьох теоретичних точок зору, таких як теорія стримування (винагороди та покарання), кримінологія та нейтралізація, оцінка страху та загрози, обізнаність та навчання інформаційній безпеці, теорія когнітивного морального розвитку, соціальні зв'язки і вплив [69].

Чи потрібно розповідати співробітникам, якою мірою ведеться контроль за їх поведінкою?

Скільки зусиль і витрат повинні понести менеджери при розгляді питань доступу до даних і конфіденційності?

Де переломний момент, за яким зусилля, спрямовані на забезпечення доступу до даних, можуть бути доступні лише тим, хто уповноважений це робити, можуть вважатися розумними та доцільними?

Чи виправдовує доступність інформації її використання?

Чи слід якимось чином обмежувати можливості організацій збирати та обробляти дані в масштабах, що експоненціально зростають?

Чи означає той факт, що інформація може бути створена з певною метою, навіть якщо таким чином індивідуальні права на конфіденційність потенційно порушуються?

Якщо дані, призначені для одного використання, перенаправляються на інший процес, який є соціально значущим і призведе до більшого блага або може призвести до фінансової вигоди, чи пом'якшує це етичну дилему, незалежно від того, наскільки невинна і чиста мотивація?

Скільки зусиль та витрат повинні понести менеджери, розглядаючи питання доступу до даних та конфіденційності?

Якого обсягу відповідальності нам слід очікувати від управителів цих даних?

Якщо сьогодні ідеального рішення не існує, де переломний момент, за яким зусилля, спрямовані на забезпечення доступу до даних і доступні лише тим, хто уповноважений це робити, можуть вважатися розумними та доцільними?

Чого роботодавці можуть очікувати від працівників у зв'язку з нерозголошенням, коли вони збираються працювати в іншу фірму?

Аналіз досліджень науковцями [67-69] застосування етичних норм та моральних проблем у кібербезпеці свідчить про те, що однозначних відповідей на ці та інші питання поки що не існує. Моральність дій залежить в кожному конкретному випадку від обставин та умов виникнення конфліктних ситуації.

Багато людей зобов'язані підписувати угоди про нерозголошення і положення про неконкуренцію в трудових договорах. Ці юридичні документи обмежують їх можливість обмінюватися інформацією з іншими майбутніми роботодавцями навіть до того, щоб заборонити їм приєднуватися до певних компаній або продовжувати брати участь в певній галузі.

А як щодо решти людей, які не мають таких законодавчих обмежень? В процесі нашої роботи для роботодавця А ми володіємо комерційною таємницею, внутрішніми документами, власними процесами і технологіями, а також іншою інформацією, що створює конкурентні переваги. Ми не можемо зробити сховище мізків та залишити отримані знання навички та сторені на їх основі технології, коли їдемо працювати до роботодавця Б; ми несемо цю інформацію з собою. Чи етично використовувати наші спеціальні знання, отримані в одного роботодавця, на благо іншого? Як реально обмежити себе в цьому?

Також існує ряд проблем щодо інтелектуальної власності.

Яка частина інформаційного активу належить організації, а що просто є частиною загальних знань працівника?

Інформація, знання та навички, які ми розвиваємо в ході роботи над проектами, можуть бути нерозривно переплетені. Ви є керівником проекту, намагаючись реінжинірингувати систему маркетингових операцій вашої компанії. Ви маєте доступ до конфіденційних внутрішніх меморандумів щодо стратегічної та процедурної інформації ключової організації. Щоб побудувати нову систему, ви та ваша команда повинні пройти поглиблене технічне навчання щодо нових технологічних продуктів, які ви будете використовувати. Нова система, яку вибудуєте, є абсолютно революційною в дизайні та виконанні. Хоча існують галузі патентного права, які охоплюють багато таких ситуацій, у юридичній практиці їх ще не так багато. Крім того, закони, в яких відображаються права інтелектуальної власності відрізняються в кожній країні.

Може статися так, що під час виконання функціональних обовязків ви створили актив, що належить вашій компанії, але чи маєте ви законні претензії

до будь-якої його частини? Чи можете ви взяти будь-яку частину цих знань або навіть сам дизайн чи код з собою іншому роботодавцю або з метою створення власної компанії? Припустимо, ви створюєте самостійно і продаєте свою розроблену програму іншим компаніям. Чи пом'якшується етична дилема тим фактом, що ваша початкова компанія не займається програмним бізнесом? Або якщо ви продали свій продукт лише неконкурентним компаніям? Що, якби ми говорили про базу даних, а не про систему?

Організації мають право стежити за тим, чим займаються співробітники і як використовуються технологічні системи. Звичайною практикою є повідомлення співробітників про те, що коли вони використовують організаційні активи, такі як мережі або доступ до Інтернету, вони не повинні очікувати конфіденційності. Навіть без цієї відмови від відповідальності їм дійсно не потрібне попередження, щоб знати, що цей моніторинг відбувається або може відбуватися.

Чи знають співробітники, наскільки відстежується поведінка?

Чи зобов'язані організації повідомляти працівників про обсяг такого моніторингу?

Чи повинна організація дати зрозуміти, що крім моніторингу того, як довго співробітники користуються Інтернетом, вона також стежить за тим, які веб-сайти вони відвідують?

Якщо організація просто каже, що не очікує конфіденційності під час використання системи електронної пошти, чи є етичним порушенням, коли співробітники пізніше дізнаються, що контролюючі органи насправді читали їхні електронні листи?

Чи порушують зібрані дані право співробітників на конфіденційність?

Багато організацій почали додавати перевірку кредитів та біографічних даних до стандартної довідкової перевірки під час процесу найму. Чи зобов'язані ці організації повідомляти нам, що вони це роблять, і які результати вони отримали? Обґрунтуванням для перевірки кредиту, як правило, є те, що людині, яка не може керувати власними фінансами, ймовірно, не можна довіряти будь-яку фідуціарну[61] відповідальність від імені організації. Це проходить перевірку на лояльність чи це насправді порушення конфіденційності?

[61] Фідуціарна і соціальна відповідальність менеджера принципово базуються на добровільному прийнятті ним обов'язку дотримання загальнолюдських етичних норм.

Виконання таких перевірок є відносно недавнім явищем, викликаним частково бажанням організацій захистити себе після численних корпоративних скандалів останніх кількох років, а також тому, що технології дозволили швидко та недорого збирати ці дані. Чи відповідає технологія за можливість неетичної поведінки?

Бізнес завжди мав стосунки любові або ненависті з точністю. Ефективне прийняття рішень обумовлене точною інформацією, але контроль якості має вартість як з точки зору витрати часу на контроль, так і продуктивності (якщо ви перевіряєте, ви також не можете робити).

Чи були перевірені системи на предмет найбільш ймовірних джерел порушення безпеки?

Раніше безпека обмежувалася замиканням дверей на виході з офісу або забезпеченням того, щоб замок на сейфі був кодований. Сьогодні технології представляють нам абсолютно новий набір викликів безпеці. Мережі можуть бути порушені, особиста ідентифікаційна інформація може бути скомпрометована, дані можуть бути викрадені і потенційно можуть призвести до фінансового краху корпорації. Критична конфіденційна корпоративна інформація або секретна державна таємниця можуть бути вкрадені з онлайн-систем, веб-сайти можуть бути зламані, реєстратори натискання клавіш можуть бути встановлені приховано та безліч інших варіантів порушень.

Як далеко може і повинно зайти керівництво у визначенні ризиків безпеки, властивих системам? Який рівень усунення цих ризиків можна вважати обґрунтованим? Яка відповідальність менеджерів та організації?

Чи можуть власники системи нести особисту відповідальність, коли безпека порушена? Коли організація здійснює управління даними про зовнішніх суб'єктів – клієнтів, фізичних осіб, інші організації – і ці дані скомпрометовані, якою мірою постраждала корпорація несе відповідальність перед вторинними жертвами, тими, чиї дані були вкрадені?

Організації, як правило, мають внутрішню політику боротьби з порушеннями безпеки, але ще не багато з них мають конкретні політики для вирішення проблем цієї сфери. Менеджери, які не забезпечують безпеку систем, за які вони несуть відповідальність, співробітники, які використовують інформацію, до якої вони не повинні мати доступу, і користувачі системи, які знаходять ярлики навколо встановлених процедур безпеки, розглядаються так само, як і будь-хто, хто не відповідає основним вимогам роботи. Рівень їх

відповідальності може бути передбачений наперед – від передачі або пониження в посаді до припинення трудового договору та адміністративної відповідальності. Критерії цієї відповідальності повинні бути визначені в угоді при прийомі на роботу, у функціональних обовязках, посадових інструкціях та у корпоративному кодексі компанії.

Шляхи вирішення потенційних моральних проблем в організації інформаційної безпеки корпорацій можуть включати:

1. Дотримання законів та регуляторних вимог з охорони персональних даних та комерційної інформації.
2. Розробка та виконання етичних стандартів для збору, зберігання та використання інформації, щоб забезпечити дотримання моральних принципів та свобод людей.
3. Застосування прозорих та відкритих процедур збору та використання інформації
4. Забезпечення безпеки та конфіденційності інформації шляхом використання сучасних технологій та захисту від кібератак.
5. Надання розуміння та навчання співробітникам щодо важливості зберігання та захисту інформації, а також створення культури безпеки даних у компанії.
6. Розробка механізмів для вирішення скарг та захисту прав співробітників та інших осіб, які можуть бути порушені при зборі та використанні інформації.
7. Підтримка відкритого та прозорого діалогу зі зацікавленими сторонами щодо питань безпеки та захисту інформації.

Таким чином, організація інформаційної безпеки корпорацій може мати потенційні моральні проблеми, які вимагають розуміння та виконання етичних стандартів та регуляторних вимог. Визначення наперед шляхів вирішення, надання навчання та створення культури безпеки даних у компанії можуть допомогти у збереженні моральних принципів та свобод людей при зборі та використанні інформації.

Крім того, корпорації повинні дотримуватися регуляторних вимог та етичних принципів, які регулюють збір, зберігання та використання інформації. Це може включати дотримання міжнародних стандартів, таких як Загальний

регламент про захист персональних даних[62] (General Data Protection Regulation або GDPR), який регулює збір та обробку персональних даних в Європейському Союзі. Також, корпорації повинні дотримуватися регуляторних вимог та етичних принципів, що стосуються захисту конфіденційної інформації, такої як банківські дані, комерційні та інтелектуальні права, державні та військові таємниці тощо.

Крім того, корпорації повинні працювати з міжнародними організаціями та урядовими установами, щоб розробляти та впроваджувати міжнародні стандарти безпеки даних та захисту приватності. Це зможе допомогти зменшити ризики порушення інформаційної безпеки та кіберзагрози. Взагалі, потенційні моральні проблеми в організації інформаційної безпеки корпорацій є важливою темою для дослідження та обговорення. Їхнє вирішення може визначити ефективність та стійкість корпорацій у сучасному інформаційному середовищі, а також їхню взаємодію з клієнтами та суспільством в цілому.

Висновок. У підсумку, врахування моральних аспектів є дуже важливим для ефективного та етичного управління інформаційною безпекою в корпораціях. Компанії повинні розглядати питання етики та моралі при прийнятті рішень щодо захисту даних та моніторингу працівників. Вони повинні відповідати перед своїми клієнтами, співробітниками та іншими зацікавленими сторонами за те, як вони збирають та зберігають дані, як вони захищають їх від втрати, крадіжки та зловживання. Важливим є також забезпечити компаніями своїм співробітникам належне навчання з питань етики та моралі, щоб вони розуміли важливість захисту даних та приватності. Також важливо забезпечити прозорість та чесність у відносинах зі співробітниками та зовнішніми зацікавленими сторонами.

Нарешті, компанії повинні враховувати потенційні моральні проблеми та виконувати етичні принципи в управлінні інформаційною безпекою. Це допоможе зберегти репутацію компанії, збільшити довіру та підвищити взаємодію з клієнтами та співробітниками.

Отже, врахування моральних аспектів та застосування етичних методів та засобів в управлінні інформаційною безпекою допоможе компаніям забезпечити високий рівень захисту даних, взаємовідносин зі співробітниками та зовнішніми зацікавленими сторонами, а також зберегти свою репутацію та довіру.

[62] Загальний регламент Європейського Союзу із захисту персональних даних (General Data Protection Regulation або GDPR) установлює важливий глобальний стандарт захисту прав на таємницю особистого життя, інформаційної безпеки та дотримання нормативно-правових вимог.

Питання для самоконтролю:

1.Які дилеми існують в кібербезпеці?

2.З якими моральними проблемами стикаються організатори кібербезпеки корпорацій?

3.Хто організує захист інформації в організації?

4.Яку відповідальність несуть порушники кібербезпеки?

Завдання:

1.Зробити аналіз 10-ти питанням Джеффа Релкіна та дати на них відповідь з моральної точки зору.

4.2. Система підтримки прийняття рішень в кібербезпеці

Сучасний розвиток технологій інформаційного суспільства вимагає відповідної уваги до питань кібербезпеки. Кіберзлочинці стають все більш винахідливими в пошуку вразливостей та атаках на інформаційні системи. Своєчасність реагування на кіберзагрози, оперативне прийняття рішення в умовах сьогодення стоїть на першому місці при організації кібербезпеки держави, установ, організацій, підприємств. Тому розробка систем підтримки прийняття рішень в кібербезпеці є дуже важливою задачею.

Кіберзагрози є більш неминучими та небезпечними, ніж будь-коли, з точки зору їх стійкості та тяжкості. Кількість порушень зросла на 15,1% з 2020 по 2021 рік. Витрати на порушення також зростають – за той же період вони підскочили на 24,5%. Більшості компаній потрібно більше шести місяців для виявлення витоків даних, включаючи такі гучні імена, як Facebook, Capital One і Equifax. Проте, понад 77% організацій не мають будь-якої форми реагування на загрози або жодного плану реагування на інциденти в області кібербезпеки, хоча більше 54% компаній вже піддавалися атакам в минулому році (згідно зі звітом компаній на зарубіжному ринку за 2020 рік).

Людський фактор і збій системи складають 52% порушень безпеки даних. Тобто головною небезпекою і головним ризиком все ще є людина – користувач

або співробітник компанії, а також програмне забезпечення, яке часто стає ненадійним за дуже короткий період часу. Навіть якщо існують базові стандартні заходи, цього навряд буде достатньо, щоб команда з безпеки знала останні загрози кібербезпеки. Оскільки характер онлайн-загроз постійно змінюється, моніторинг аналітики загроз має вирішальне значення для будь-якого бізнесу. Саме тому більшість фахівців інформаційної безпеки рекомендують підключати послугу цілодобового моніторингу та аналізу і запроваджувати системи підтримки прийняття рішення для своєчасного реагування на загрози в інформаційних системах.

Існує безліч видів розвідки загроз. Їх розділяють на три категорії.

Стратегічний аналіз загроз в кібербезпеки. Стратегічна розвідка загроз використовує дані з відкритих джерел, що означає, що вони можуть бути легко доступні громадськості. Сюди входять національні та місцеві засоби масової інформації, звіти, рейтинги безпеки, онлайн-активність, онлайн-статті та офіційні документи. Зазвичай такий аналіз використовується для не технічної аудиторії, включно з членами ради директорів або зацікавлених осіб, і інформує їх про елементи, такі як оцінки безпеки або навіть можливий вплив бізнес-рішень.

Тактичний аналіз. Цей тип аналізу загроз зосереджений на тому, що може статися в найближчому майбутньому. Це допомагає командам з безпеки визначити, чи будуть існуючі програми успішно виявляти та уникати загроз. Коли справа доходить до розвідки загроз, тактична розвідка загроз є основною формою, оскільки вона є автоматичною і найпростішою з усіх генерованих. Це дозволяє компаніям визначати, наскільки ймовірно, що вони будуть атаковані, ґрунтуючись на методах, які використовуються хакерами.

Оперативний аналіз. Оперативна розвідка загроз аналізує минулі атаки і відповідає на всі істотні питання, такі як хто, як, що, коли. Вивчаючи минулі атаки, легше зрозуміти, як і коли можуть відбутися майбутні атаки.

Тип інформаційної системи, яку використовує користувач, залежить від їх рівня в організації. На схемі (рис. 4.1) нижче показано три основні рівні користувачів в організації та тип інформаційної системи, яку вони використовують.

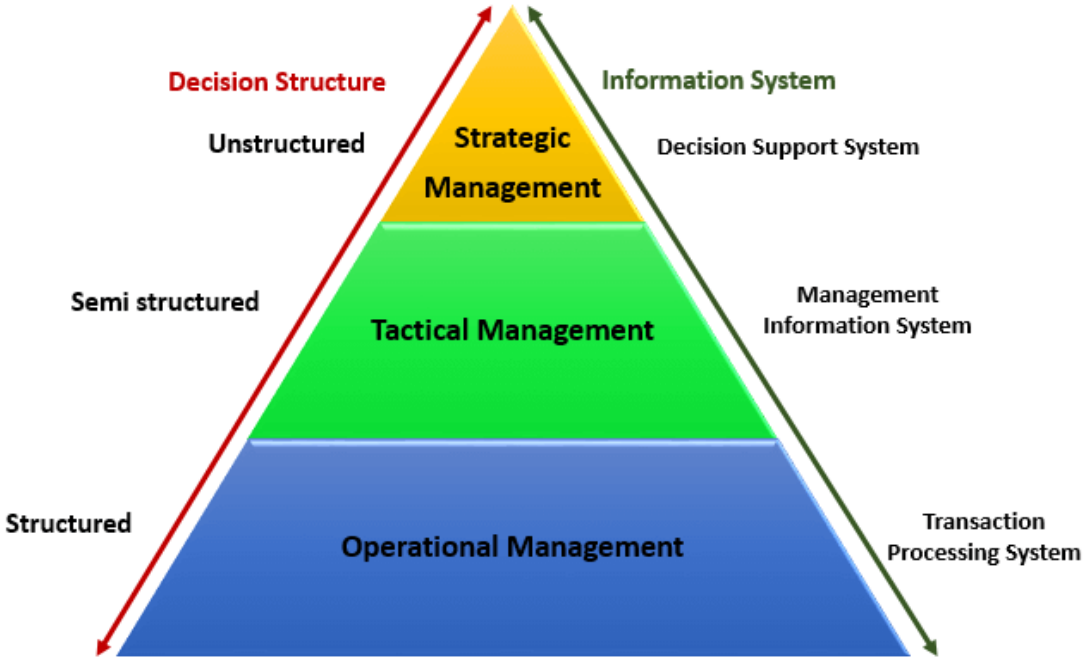


Рис. 4.1. Рівні і типи інформаційних систем

Системи обробки транзакцій[63] (англ. Transaction processing system – TPS). Цей тип інформаційної системи використовується для обліку повсякденних операцій бізнесу. Прикладом системи обробки транзакцій є система точок продажу (POS). Для запису щоденних продажів використовується POS-система.

Управлінські інформаційні системи (англ. Management information systems MIS) використовуються для керівництва менеджерами-тактиками прийняття напівструктурованих рішень.

Завданням таких систем є допомога фахівцю або керівництву кібербезпеки у прийнятті зважених ефективних рішень.

Системи підтримки прийняття рішень (СППР) – це особливі інтерактивні системи, які використовують обладнання, програмне забезпечення, дані, базу моделей і роботу менеджера з метою підтримки всіх стадій прийняття рішень у процесі аналітичного моделювання. Іншими словами, система підтримки прийняття рішень - комплекс програмних засобів, що включає комплекс різних алгоритмів підтримки рішень, базу моделей, базу даних, допоміжні та керівну програми. Керівна програма забезпечує процес прийняття рішень з урахуванням

[63] Транза́кція (англ. transaction) – група послідовних операцій з базою даних, яка є логічною одиницею роботи з даними. Транзакція може бути виконана або цілком і успішно, дотримуючись цілісності даних і незалежно від інших транзакцій, що йдуть паралельно, або не виконана зовсім, і тоді вона не може справити ніякого ефекту. Транзакції оброблюються транзакційними системами, в процесі роботи яких створюється історія транзакцій.

специфіки проблеми. СППР використовується для підтримки різних видів діяльності у процесі прийняття рішень, а саме для:

- полегшення взаємодії між даними, процедурами аналізу й обробки даних і моделями прийняття рішень, з одного боку, та особи, що приймає рішення, як користувача цих систем – з іншого;
- надання допоміжної інформації, особливо для виконання не-структурованих або слабоструктурованих завдань, для яких важко заздалегідь визначити дані та процедури відповідних рішень.

Таким чином СППР складається з двох основних підсистем – це люди, що приймають рішення, і комп'ютерна система.

В роботі [70] зроблений аналіз можливостей існуючих СППР, який зведений у таблицю 4.1.

Таблиця 4.1

Порівняння можливостей сучасних СППР

Назва СППР	Реалізовані методи	Парні порівняння	Часовий аналіз	Аналіз чутливості	Групове оцінювання	Наявність різних шкал	Наявність веб-версії
1000Minds	PAPRIKA	Так	Ні	Так	Так	Ні	Так
AIRM Online	AIRM	Ні	Ні	Так	Ні	Ні	Так
Analytica		Ні	Так	Так	Ні	Ні	Так
DecisionLab		Так	Ні	Так	Ні	Ні	Ні
DecisionLens	AHP, ANP	Так		Так	Так		Так
D-Sight	MAUT, PROMETHEE	Так	Ні	Так	Так	Ні	Так
ExpertChoice	AHP	Так	Ні	Так	Так	Ні	Так
LogicalDecisions	AHP, MAUT	Так	Ні	Так	Так	Ні	Ні
MakeItRational	AHP	Так	Ні	Так	Так	Ні	Так
MindDecider	AHP	Ні	Так	Так	Так	Ні	Ні
PROMETHEE Visual	PROMETHEE	Так	Ні	Так	Так	Так	Ні
RFP	AHP, ANP	Так	Так	Так	Так	Ні	Так
SuperDecisions	AHP, ANP	Так	Ні	Так	Ні	Ні	Ні
TreeAgePro		Ні	Ні	Так	Ні	Ні	Ні
VeryGoodChoice	ELECTRE	Так	Ні	Так	Так	Ні	Ні
ОЦІНКА И ВИБІР	АНР, ФЦ, ПаретоАн	Так	Ні		Так	Ні	Так

Назва СППР	Реалізовані методи	Парні порівняння	Часовий аналіз	Аналіз чутливості	Групове оцінювання	Наявність різних шкал	Наявність веб-версії
СВИРЬ	БКОпт, Класиф, АНР	Так	Ні	Так	Так		Ні
СОЛОН	МЦДОА	Так	Так	Так	Так	Так	Так

Системи підтримки прийняття рішень в кібербезпеці (СППРК) - це програмні комплекси, що надають інформаційну підтримку прийняттю рішень в галузі кібербезпеки. Вони допомагають аналізувати потенційні загрози, виявляти уразливості та розробляти стратегії захисту.

Однією з найважливіших функцій СППРК є аналіз потенційних загроз. Для цього використовуються різноманітні методи, такі як аналіз ризиків, оцінка вразливостей, моніторинг та аналіз подій тощо. Важливою складовою СППРК є інтелектуальна система аналізу даних, яка дозволяє автоматично виявляти потенційні загрози та уразливості.

Ще одна важлива функція СППРК - це планування заходів забезпечення кібербезпеки. Система може автоматично генерувати рекомендації щодо захисту від потенційних загроз, а також розробляти стратегії забезпечення кібербезпеки на основі аналізу інформації про попередні атаки та загрози.

СППРК можуть бути класифіковані за багатьма критеріями. Одним з них є характер вхідних даних, що обробляються системою. Наприклад, системи, що обробляють дані з мережі, можуть бути класифіковані як системи детекції або виявдення вторгнень (IDS), а системи, що обробляють дані з лог-файлів, можуть бути класифіковані як системи детекції витоку даних (DLP).

Інший критерій класифікації - це рівень автоматизації системи. Деякі СППРК можуть бути повністю автоматизовані та не потребувати участі користувача, тоді як інші можуть бути напівавтоматизовані та вимагати участі користувача в процесі прийняття рішень.

СППРК можуть бути розроблені з використанням різних методів штучного інтелекту, таких як машинне навчання, генетичний алгоритм, еволюційні алгоритми, нейронні мережі та експертні системи. Кожен з цих методів має свої переваги та обмеження, тому вибір конкретного методу залежить від конкретних потреб користувачів та вимог до СППРК.

Машинне навчання є одним з найбільш ефективних методів для розробки СППРК. З його допомогою можна навчити систему розпізнавати типи атак та виявляти уразливості. Машинне навчання може бути використане для автоматичного виявлення аномальної поведінки в мережі, що може свідчити про атаку. Генетичний алгоритм може використовуватись для пошуку оптимальних параметрів системи захисту від потенційних загроз. Крім того, можна використовувати навчання з підкріпленням для автоматичного визначення оптимальних стратегій захисту.

Експертиза для оцінки рівня безпеки конкретної IT-системи зазвичай недоступна в одному місці. Крім того, знання про вразливості в системах швидко розвиваються, що робить необхідним для організацій підтримувати актуальну обізнаність про потенційну експозицію своїх систем. В цих умовах потрібний новий підхід з метою фіксації та інтеграції оцінок безпеки, включаючи пов'язану з цим невизначеність з багатьох джерел, до яких би входили державні служби, приватні підприємства і організації та навчальні заклади, а також сторонні постачальники безпеки. Ключова проблема тут полягає в тому, щоб розробити способи ефективного збору та моделювання цієї часто складної інформації, а також систематично боротися з різними поглядами в оцінках безпеки, наданих окремими джерелами.

Однак, існує декілька викликів, які потрібно вирішити в процесі розробки та впровадження СППРК. Перш за все, необхідно забезпечити точність та достовірність вхідних даних, оскільки неправильна інтерпретація даних може призвести до неправильного прийняття рішень. Крім того, необхідно забезпечити захист від атак, які можуть бути спрямовані на саму СППРК.

Ще один важливий виклик полягає у тому, що СППРК мають справу з великою кількістю даних та інформації. Це може створити проблему з пам'яттю та обробкою даних в реальному часі. Для подолання цього виклику можуть використовуватись методи компресії даних та інші методи оптимізації.

У майбутньому розвиток СППРК буде спрямований на поліпшення точності та швидкості обробки даних, розширення функціональності та забезпечення відповідності з стандартами кібербезпеки. Також можна очікувати розвитку більш складних алгоритмів та технологій машинного навчання, які дозволять покращити ефективність СППРК.

У підсумку, СППРК стають все більш важливими в забезпеченні безпеки інформаційних систем в різних галузях. Використання методів штучного

інтелекту може допомогти покращити ефективність та швидкість роботи СППРК, що зробить їх ще більш важливими в боротьбі з кіберзлочинами.

Системи підтримки прийняття рішень в кібербезпеці є важливим інструментом для забезпечення безпеки інформаційних систем в різних галузях. Однак, наявність таких систем також породжує етичні питання та проблеми, пов'язані з їх застосуванням. розглянуті етичні принципи застосування СППР в кібербезпеці та їх важливість для забезпечення справедливого та етичного застосування цих систем забезпечить врахування моральних цінноістей.

Етичні принципи застосування СППР в кібербезпеці

Принцип прозорості та відповідальності. Системи підтримки прийняття рішень в кібербезпеці повинні бути прозорими та відповідальними. Це означає, що розробники та користувачі СППР повинні забезпечити доступність та зрозумілість процесу прийняття рішень. Крім того, користувачі повинні бути повністю бути відповідальні за будь-які наслідки прийнятих рішень. Це може бути досягнуто шляхом встановлення чітких процедур контролю та відповідальності, а також шляхом надання детальної документації щодо процесу прийняття рішень.

Принцип відсутності дискримінації та нерівності. Системи підтримки прийняття рішень в кібербезпеці повинні бути бездискримінаційними та спрямовуватися на забезпечення однаково рівної обробки даних для всіх користувачів. Це означає, що СППР не повинні бути налаштовані на прийняття рішень на підставі расової, етнічної або соціальної приналежності, статі, орієнтації на стать або будь-яких інших особистих характеристик користувача. Крім того, СППР повинні бути спрямовані на забезпечення рівності можливостей та доступу до інформації для всіх користувачів.

Принцип приватності та захисту даних. Системи підтримки прийняття рішень в кібербезпеці повинні дотримуватись принципу приватності та захисту даних. Це означає, що системи повинні забезпечувати безпеку та конфіденційність даних користувачів, використовувати мінімально необхідну кількість інформації та відповідати найвищим стандартам безпеки. Крім того, СППР повинні бути сумісні з відповідними нормами та законами щодо захисту персональних даних та конфіденційності.

Принцип адаптивності та гнучкості. Системи підтримки прийняття рішень в кібербезпеці повинні бути адаптивними та гнучкими. Це означає, що системи повинні мати можливість змінюватись та адаптуватись до мінливих

умов та потреб користувачів. Крім того, СППР повинні бути гнучкими у виборі алгоритмів та методів прийняття рішень, що дозволяє їх використовувати в різних сферах кібербезпеки.

Принцип етики та доброчесності. Системи підтримки прийняття рішень в кібербезпеці повинні дотримуватись принципів етики та доброчесності. Це означає, що розробники та користувачі повинні дотримуватись етичних норм та стандартів у процесі розробки, використання та вдосконалення СППР. Крім того, СППР повинні сприяти збереженню та зміцненню довіри до кібербезпеки, забезпечувати чесність та прозорість прийнятих рішень та не допускати дискримінації користувачів на основі етичних, соціальних чи інших причин.

Принцип доступності та простоти. Системи підтримки прийняття рішень в кібербезпеці повинні бути доступними та простими у використанні. Це означає, що СППР повинні бути доступні для широкого кола користувачів, незалежно від їх технічних знань та досвіду. Крім того, СППР повинні мати інтуїтивно зрозумілий та легкий у використанні інтерфейс, що дозволяє користувачам швидко та ефективно вирішувати проблеми кібербезпеки.

Результати досліджень показують, що використання систем підтримки прийняття рішень в кібербезпеці буде позитивно впливати на зниження кіберзагроз та ризиків. Однак, для досягнення найкращих результатів необхідно дотримуватись етичних принципів та враховувати важливість захисту прав та свобод користувачів.

У практичному плані, етичні принципи застосування СППР в кібербезпеці можуть бути реалізовані шляхом розробки етичного кодексу для розробників та користувачів СППР, використання етичних аудитів та рецензій для оцінки дотримання етичних стандартів, а також залучення етичних експертів до процесу розробки та вдосконалення СППР.

Зокрема, в кодексі мають бути визначені вимоги до захисту приватності персональних даних, заборону використання СППР для дискримінації або порушення прав людини, необхідність врахування можливих наслідків та ризиків при прийнятті рішень, а також вимоги до відповідальності та прозорості в діях розробників та користувачів СППР.

Важливо також зазначити, що етичні принципи застосування СППР в кібербезпеці не повинні перешкоджати розробці та впровадженню нових технологій та рішень, а лише забезпечувати їх відповідність вимогам моралі та права. Також важливо розуміти, що етичні принципи не є статичними, а мають

підлягати постійному вдосконаленню та адаптації до змін у суспільстві та технологіях.

Сьогодні у світі створені багато моделей з етичними складовими, які допомагають управлінцям приймати рішення. Американська модель зображена на рис. 4.2.

Рис. 4.2. Американська модель етичного прийняття рішень

На рисунку 4.2 зображено модель етичного прийняття рішень, яка відображає основні етапи та фактори, що впливають на етичне прийняття рішень в контексті застосування СППР в кібербезпеці. Перший етап - це збір інформації та визначення проблеми. Другий етап полягає у формулюванні альтернативних рішень та їх аналізі. На третьому етапі приймається рішення на основі аналізу альтернатив та здійснюється відповідальне виконання прийнятого рішення. Четвертий етап - це оцінка та контроль результатів, а також їх відповідність етичним принципам та стандартам. В результаті проводиться кінцевий вибір.

Для порівняння на рис. 4.3 наведена українська модель прийняття рішення.

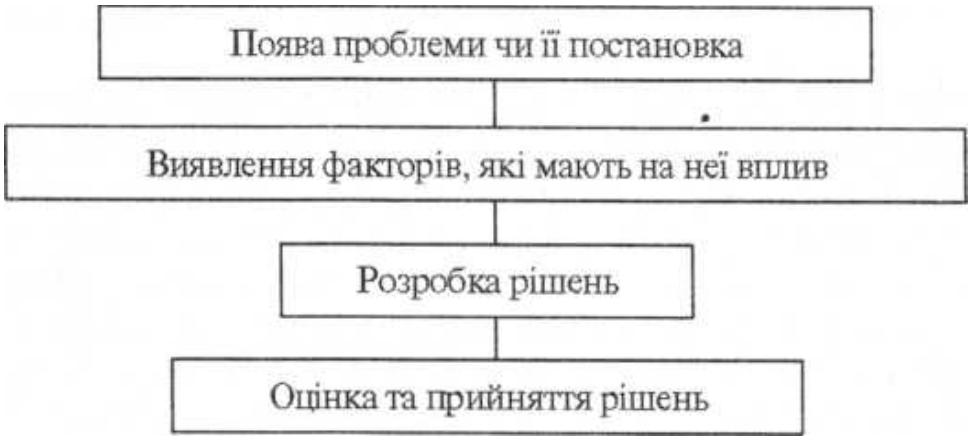


Рис. 4.3. Українська модель прийняття рішення

Висновки. Системи підтримки прийняття рішень в кібербезпеці стають все більш важливими у зв'язку зі зростаючими загрозами від кіберзлочинців. Вони дозволяють автоматизувати процеси аналізу потенційних загроз та розробки стратегій захисту. Інтеграція методів штучного інтелекту дозволяє покращити ефективність СППРК та забезпечити їх адаптацію до змінних умов кібербезпеки. Такі системи стають невід'ємною складовою інфраструктури кібербезпеки та грають ключову роль у забезпеченні безпеки інформації в сфері бізнесу, урядів та інших організацій, що залежать від безпеки своїх інформаційних систем.

Розробка та використання СППР в кібербезпеці повинні ґрунтуватися на етичних принципах та відповідальному підході до прийняття рішень. Етичні принципи повинні бути вбудовані в процес розробки та використання СППР, а також підлягати постійному вдосконаленню та адаптації до змін у суспільстві та технологіях. Важливо забезпечити дотримання етичних принципів при розробці та використанні СППР, що дозволить забезпечити захист прав та свобод людини, забезпечити конфіденційність та безпеку даних, а також підвищити довіру до технологій кібербезпеки.

Питання для самоконтролю:

1.На якому рівні інформаційних систем застосовують СППР?

2.Що включає СППР?

3.Які СППР застосовуються у кібербезпеці?

Завдання:

1.Оцінити можливість застосування SuperDecisions, DecisionLens, D-Sight, Promethee у кібербезпеці.

4.3. Етичні методи і засоби управління інформаційними інцидентами і ризиками.

Етика управління інформаційними інцидентами і ризиками пов'язана зі збереженням та захистом інформації від несанкціонованого доступу, її використання та поширення. Основні принципи етики управління

інформаційними інцидентами і ризиками включають конфіденційність, цілісність та доступність інформації.

У сучасному світі, де інформаційні технології стали невід'ємною частиною життя людей і підприємств, суспільства і держави, захист інформації стає ключовим завданням. Однак, на жаль, інформаційні інциденти і ризики все ще є досить поширеними явищами. Тому, етичні методи і засоби управління інформаційними інцидентами і ризиками виконують важливу роль у забезпеченні захисту інформації та зниженні впливу негативних наслідків таких інцидентів на підприємства, організації та користувачів.

Жоден найдосконаліший спосіб зниження ризиків інформаційної безпеки, будь це політика безпеки, що досконально опрацьована, або найсучасніший брандмауер, не може захистити від виникнення в інформаційному середовищі подій, що потенційно несуть загрозу діяльності організації. Складність і різноманітність середовища діяльності сучасних підприємств і організацій зумовлюють наявність залишкових ризиків незалежно від якості підготовки і впровадження заходів протидії. Також завжди існує вірогідність реалізації нових, невідомих до теперішнього часу, загроз інформаційній безпеці. Неготовність організації до обробки подібного роду ситуацій може істотно ускладнити відновлення бізнес-процесів та потенційно збільшити завдані збитки.

Кількість потенційних каналів витоку інформації достатньо велика. Найбільш поширені з них відносяться до категорії ненавмисного розкриття інформації співробітниками організації з причин непоінформованості або недисциплінованості. Відсутність уявлень щодо правил роботи з конфіденційними документами, невміння визначити, які документи є конфіденційними, та звичайна неуважність при роботі з інформацією – все це може призвести до виникнення події або інциденту інформаційної безпеки.

Велику групу організаційних методів управління інформаційними ризиками становлять методи застосування засобів управління ризиками. Для реалізації даних методів управління розробляються методики, інструкції, графіки, схеми, правила, функціональні обов'язки, які дозволяють персоналу застосовувати засоби управління інформаційними ризиками [70-72]. Один із варіантів схеми управління ризиками показаний на рис. 4.4.

Рис.4.4. Схема організації управління ризиками.

Управління ризиками інформаційної безпеки повинно здійснюватись з дотриманням етичних принципів та правил. Деякі з етичних методів застосування засобів управління ризиками інформаційної безпеки включають в себе наступне:

1. Дотримання законодавства: організації мають дотримуватись законодавства та регуляторних вимог в галузі інформаційної безпеки. Це допомагає запобігти порушенням прав користувачів, а також забезпечує належний рівень захисту конфіденційної інформації.

2. Транспарентність[64]: організації мають дотримуватись прозорості у своїй діяльності та інформувати користувачів про можливі ризики, пов'язані з обробкою їх персональних даних.

3. Мінімізація даних: організації повинні збирати та зберігати лише необхідну кількість даних для забезпечення своїх функцій та послуг. Це допомагає запобігти можливим порушенням даних та зменшує ризики.

4. Розробка та впровадження політики інформаційної безпеки: організації мають розробляти та впроваджувати політику інформаційної безпеки, яка визначає процедури та правила для збереження, обробки та передачі даних. Це

[64]Транспарентність, -ності, ж. Вірогідність, ясність і можливість легкої перевірки відомостей про що-небудь; відсутність таємності.

допомагає забезпечити належний рівень захисту даних та запобігти їх порушенням.

5. Навчання та свідоме користування: організації мають надавати своїм співробітникам та користувачам достатню освіту та навички, щоб забезпечити сві доме користування та безпеку використання інформаційних технологій. Це може включати навчання з принципів безпеки даних, захисту від шахрайства та фішингу, а також свідоме використання паролів та інших методів аутентифікації.

6. Захист конфіденційної інформації: організації повинні забезпечувати належний рівень захисту конфіденційної інформації. Це може включати застосування шифрування даних, мережевого захисту та інших методів, щоб запобігти несанкціонованому доступу до конфіденційної інформації.

7. Відповідальне використання даних: організації повинні використовувати зібрані дані тільки для своїх законних цілей та не повинні передавати їх третім особам без дозволу власника даних. Це допомагає запобігти зловживанням зібраними даними та порушенням приватності користувачів.

8. Аналіз та оцінка ризиків: організації повинні регулярно аналізувати та оцінювати ризики, пов'язані з їхніми інформаційними системами та даними. Це допомагає виявляти можливі загрози та вживати заходів щодо запобігання їх реалізації.

9. Повідомлення про потенціальні події і інциденти: організації мають повідомляти користувачів та інші сторіни про можливі інциденти, пов'язані з їхніми даними. Це допомагає забезпечити відкритість та довіру між організаціями та учасниками.

Під подією інформаційної безпеки (ПІБ) розуміється стан системи, сервісу або мережі, котрий свідчить про можливе порушення політики безпеки, або про невідому ситуацію, яка може мати відношення до безпеки. Під подією також розуміють ідентифікований випадок стану системи або мережі, який вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту, або раніше невідому ситуацію, яка може бути суттєвою для політики безпеки.

Інцидент інформаційної безпеки (ІІБ) – це одна подія або серія подій інформаційної безпеки, які можуть призвести до збитків та втрат для організації. Втрати можуть бути, як матеріальними (вартість інформації, експлуатаційні витрати і т.д.) так і нематеріальними (репутація організації, зміна морально-психологічного клімату і т.д.) .

Як приклад, інцидентами інформаційної безпеки, що сталися з вини співробітників можуть бути:

- порушення конфіденційності та цілісності цінної інформації;
- незаконний моніторинг інформаційних систем;
- знищення інформації;
- компрометація інформаційної системи (наприклад, розголошення пароля користувача);
- відмова в обслуговувані сервісів, засобів обробки інформації, обладнання;
- пошкодження електричних мереж;
- неавторизоване використання системи для зберігання особистих даних;
- та інші порушення вимог до інформаційної безпеки, прийнятих в компанії (порушення правил обробки інформації).

Для того, щоб захистити організацію від витоку конфіденційної інформації через її співробітників, потрібно:

- контролювати доступ співробітників до закритої документації і до баз даних, кожен співробітник незалежно від свого службового положення повинен володіти лише тією інформацією, яка йому потрібна для роботи;
- періодично продивлятися данні та визначати ступінь їх секретності;
- зберігати важливу інформацію у вогнестійких сейфах, оснащених кодовим замком. Необхідно організовувати систему класифікації з обмеженим доступом різних категорій співробітників, які пройшли спеціальну перевірку;
- встановити на всіх персональних комп’ютерах антивірусні програми та регулярно їх обновлювати;
- упорядкувати використання співробітниками копіювальної техніки;
- встановити апарат для знищення непотрібних документів(включаючи використаний копіювальний папір);
- встановити персональну відповідальність співробітників за збереження конфіденційної інформації з чіткою градацією мір дисциплінарного та морального впливу за її витік.

В багатьох компаніях відсутня процедура управління інцидентами, тому не завжди є можливість прослідкувати за зміною кількості та характеру ІІБ.

Зазвичай відсутність інцидентів ще не вказує на те що система управління безпекою працює правильно, а вказує лише на те, що інцидент не фіксується.

В загальному випадку, ознаки інциденту поділяються на дві основні категорії: повідомлення про те, що інцидент відбувається в даний момент і повідомлення про те, що інцидент, можливо, станеться в недалекому майбутньому.

Для опису процедури управління інцидентами безпеки використовується класична модель безперервного поліпшення процесів, що отримала назву від циклу Шухарта-Демінга (рис. 4.3) – модель ПРПД (Плануй(Plan) – Роби(Do) – Перевіряй(Check) – Дій(Act), називають скоросено модель PDCA)

Рис. 4.5. Цикл Шу́харта-Де́мінга – модель безперервного поліпшення процесів

При розслідуванні інциденту збір даних може бути виконаний з допомогою програмного забезпечення "Disk Duplicate", яке дозволяє зробити точні копії жорстких дисків ("сектор в сектор") автоматизованих робочих місць користувачів (співробітників компанії) і серверів. Для аналізу отриманих даних можуть використовуватися спеціальні засоби емуляції робочих машин користувачів, наприклад "VMware Virtual Machine". Аналіз просторів жорстких дисків може проводитися з використанням спеціалізованого програмного продукту "Encase Enterprise Edition" або експертних засобів компанії Vogon International. Ці два продукти - ключові в світі при проведенні розслідування інцидентів ІБ. У ряді випадків для виявлення слідів комп'ютерних інцидентів можуть бути використані всілякі програмно-апаратні комплекси для

"прослухування" локальній мережі компанії (часто використовується продукт Ettercap - мережевий сніффер).

На етапі розслідування інцидентів важливу роль відіграють: ведення журналів реєстрації подій, чітке розділення повноважень користувачів, відповідальність за виконані дії – важливі докази того, хто брав участь в інциденті і які дії він виконував.

Типовою практикою є ведення журналу розслідування інциденту, який поки що не має стандартної форми і розроблюється командою реагування.

Ключовими позиціями подібних журналів є:

- статус розслідування, який є на даний момент;
- опис інциденту;
- дії, проведенні командою реагування в процесі обробки ІІБ;
- перелік свідоцтв (з обов'язковою вказівкою джерел), зібраних в процесі обробки інциденту;
- коментарі учасників розслідування інциденту;
- опис послідуючих дій.

Для підвищення ефективності розслідування інцидентів інформаційної безпеки в організації повинен бути інженер з інформаційної безпеки, що буде:

- розробляти політики безпеки (ПБ) з детально опрацьованими документами, які регламентують діяльність персоналу всіх рівнів з чітко вказаною відповідальністю в межах покладених обов'язків;
- розробляти посадові інструкції, правила, регламенти з чітко визначеними правами та обов'язками персоналу, пов'язані з текучими бізнес-процесами, що дозволяють добре прогнозувати наслідки та розробити надійні превентивні дії для запобігання повторення таких інцидентів.

В організації повинен бути розроблений відповідний дисциплінарний процес, що проводиться по відношенню до порушників безпеки і передбачує розслідування наслідків інцидентів та прийняття адекватних мір впливу на них.

При визначені міри запобігання виникненню інцидентів інформаційної безпеки, інженеру з інформаційної безпеки або юристу, необхідно орієнтуватися на положення дійсного законодавства України. Відносини між робітником та роботодавцем та відповідальність за порушення інформаційної безпеки організації регулюються Кримінальним Кодексом, Адміністративним Кодексом та Кодексом Законів про Працю:

1. За шкоду, заподіяну підприємству, установі, організації при виконанні трудових обов'язків, працівники, з вини яких заподіяно шкоду, несуть матеріальну відповідальність у розмірі прямої дійсної шкоди, але не більше свого середнього місячного заробітку.

2. Умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності, -- караються штрафом від двохсот до тисячі неоподаткованих мінімумів доходів громадян або обмеженням волі на строк до п'яти років, або позбавленням волі на строк до трьох років.

3. Умисне розголошення комерційної або банківської таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності, - карається штрафом від двохсот до п'ятисот неоподатковуваних мінімумів доходів громадян з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років, або виправними роботами на строк до двох років, або позбавленням волі на той самий строк.

4. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах, або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, - караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи.

5. Здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в автоматизованих системах, - тягне за собою накладання штрафу від п'яти до десяти неоподатковуваних мінімумів доходів громадян з конфіскацією засобів, що використовувалися для незаконного доступу, або без такої.

На жаль, про розслідування інцидентів в компаніях часто просто забувають. Як тільки наслідки інциденту усунені, і бізнес-процеси відновлені,

подальші дії з розслідування інциденту і здійснення коригуючих заходів не виконуються.

Сьогодні важливу роль відіграють Групи реагування на інциденти, пов'язані з комп'ютерною безпекою (CSIRT), або команда управління інцидентами (IMT). Вони часто призначаються заздалегідь або під час інциденту, і керують організацією під час розгляду інциденту для відновлення нормальних функцій. Наприклад, якщо організація виявить, що зловмисник отримав несанкціонований доступ до комп'ютерної системи, CSIRT проаналізує ситуацію, визначить величину та застосує коригувальні заходи.

В корпораціях та великих державних організаціях створюється система управління інцидентами в кібербезпеці (Cyber Incident Management System, CIMS) - організаційна структура та процеси, які використовуються для управління і відновлення після кіберінциденту, такого як кібератака, крадіжка даних, або інші подібні ситуації. Основною метою CIMS є забезпечення ефективного та швидкого відновлення роботи інформаційної системи та зниження шкоди від інциденту. Вона повинна мати наступні компоненти:

1. Керівництво та управління: Система має чітко визначену структуру керівництва, яка включає в себе керівника команди реагування на кіберінцидент, Штаб оперативного управління (ШОУ), та інші рольові групи.

2. Комунікації: CIMS вимагає наявності ефективної системи комунікацій для забезпечення передачі інформації між різними рівнями керівництва та іншими зацікавленими сторонами.

3. Оцінка ситуації: CIMS включає процес оцінки ситуації, який допомагає визначити рівень загрози та ризиків для інформаційної безпеки.

4. Планування та управління ресурсами: Система CIMS вимагає ретельного планування та управління ресурсами для забезпечення ефективного відновлення після кіберінциденту.

5. Дії на місці події: Цей компонент включає в себе дії на місці події, які здійснюються відповідно до розробленого плану дій для відновлення роботи інформаційної системи та усунення наслідків кіберінциденту. Цей компонент також включає в себе реагування на інцидент, встановлення контролю над ситуацією, збір та аналіз інформації, відновлення роботи системи та усунення наслідків кіберінциденту.

6. Аналіз та звітність: Останнім елементом складу CIMS є процес аналізу та звітності, який допомагає зрозуміти причини інциденту та вжити заходів для запобігання подібних інцидентів у майбутньому.

У кібербезпеці важливо розробити і реалізувати CIMS для ефективної відповіді на кіберінциденти та забезпечення безпеки та захисту важливих даних. Реалізація системи управління інцидентами допомагає підвищити рівень безпеки і захисту інформації та зменшити можливі витрати на відновлення після кіберінциденту.

Етичне управління інформаційними інцидентами та ризиками включає в себе декілька ключових методів та засобів.

Перший метод полягає в тому, щоб забезпечити чіткість та прозорість в управлінні інформаційними ризиками. Це можна досягти шляхом встановлення внутрішніх правил та процедур для збору, зберігання та обробки інформації, а також використання спеціальних програмних засобів для моніторингу та виявлення потенційних загроз.

Другий метод полягає в розробці відповідних стратегій для реагування на інциденти та ризики. Це включає в себе розробку планів невідкладних заходів, щоб уникнути негативних наслідків, а також встановлення процедур для виявлення, оцінки та повідомлення про інциденти. Важливо також розробити методику оцінки ризиків та встановити процедури для виявлення нових загроз та попереднього їх аналізу.

Третій метод полягає в підготовці персоналу до відповідного рівня компетенції та кваліфікації. Це включає навчання співробітників правилам інформаційної безпеки, використання захисних технологій, а також підготовку до реагування на інциденти. Крім того, важливо забезпечити взаємодію з іншими департаментами, які можуть бути залучені до управління інформаційними інцидентами, наприклад, з юридичним відділом для вирішення питань юридичної відповідальності, з відділом з розробки програмного забезпечення для виявлення технічних проблем тощо.

Четвертий метод полягає в підвищенні свідомості користувачів щодо правил інформаційної безпеки. Це можна забезпечити шляхом проведення навчальних курсів та тренінгів для користувачів, що допоможе їм уникати загроз та захистити свою інформацію. Важливо також забезпечити відповідну інформаційну підтримку користувачів у разі інцидентів.

П'ятий метод полягає в розробці етичних кодексів поведінки для співробітників і користувачів. Це включає в себе встановлення правил поведінки, які враховують етичні принципи та стандарти, що пов'язані з інформаційною безпекою та захистом даних. Етичний кодекс поведінки допоможе сприяти свідомій поведінці співробітників та користувачів, що відповідає вимогам інформаційної безпеки.

Державна регламентація управління інформаційними ризиками проводиться на підприємствах банківської системи, підприємствах з критичними виробничими процесами, що становлять загрозу населенню та навколишньому середовищу у разі аварійних ситуацій. Навіть якщо підприємство не підпадає під дію нормативних актів про обов'язкове регулювання заходів з управління окремими інформаційними ризиками, також доцільно використовувати сертифіковані засоби управління і застосовувати механізми управління, оскільки відповідність рекомендаціям стандартів дозволяє створити збалансовану, близьку до оптимальної системи управління інформаційними ризиками. Одним із прикладів регламентації управління інформаційними ризиками з урахуванням міжнародних стандартів є застосування Платформи для підвищення кібербезпеки критично важливих інфраструктур, розробленої Національним інститутом стандартів і технологій у 2018 році [72].

Висновок. Отже, етичні методи і засоби управління інформаційними інцидентами та ризиками є дуже важливими для забезпечення захисту інформації та зниження впливу інформаційних загроз на організацію. Реалізація цих методів дозволяє забезпечити відповідний рівень захисту даних та знизити ризики від інформаційних інцидентів з урахуванням моральних принципів суспільства.

Однак, важливо зазначити, що успішне впровадження етичних методів та засобів управління інформаційними інцидентами та ризиками залежить від ряду факторів. Перш за все, важливо мати відповідні ресурси та фінансову підтримку для розробки та впровадження необхідних заходів. Крім того, важливо забезпечити взаємодію з різними департаментами організації, що може бути складним завданням в більшості випадків.

Також слід зазначити, що етичні методи та засоби управління інформаційними інцидентами та ризиками не можуть забезпечити 100% захисту від інформаційних загроз. Важливо забезпечити постійне оновлення та покращення систем безпеки з метою зниження ризиків від інформаційних загроз.

Етичні методи та засоби управління інформаційними інцидентами та ризиками є важливою складовою частиною інформаційної безпеки організацій. Розробка та впровадження етичних методів та засобів дозволяє забезпечити відповідний рівень захисту даних та зменшити ризики від інформаційних інцидентів з урахуванням моральних цінностей суспільства та етичної поведінки членів організації.

Питання для самоконтролю:

1. Яке завдання CSIRT?
2. На що потрібно орієнтуватись При визначені міри запобігання виникненню інцидентів ІБ?
3. Що повинен розробляти інженер з інформаційної безпеки для підвищення ефективності розслідування інцидентів інформаційної безпеки в організації?
4. Який зміст журналу розслідування інциденту?
5. В чому суть процедури управління інцидентами безпеки?

Завдання:

1. Наведіть приклад інцидентів інформаційної безпеки, що можуть сталися з вини співробітників.

СПИСОК ЛІТЕРАТУРИ

1. Тофтул М.Г. Етика: підручник. Житомир: Вид-во ЖДУ ім. І. Франка, 2010. 448 с.
2. В. Ставнюк. Арістотель. Нікомахова етика / Αριστοτελους. Ηθικα Νικομαχεια. – К.: Аквілон-Плюс, 2002. 480 с. (переклад з давньогрецької, коментарі).
3. Сенека. Про блаженне життя. - К.: Либідь, 1994. – 128 с..
4. С. А. Ошеров. Сенека: від Риму до світу/Луцій Анней Сенека. Моральні листи до Луцилія./ Пер. і прим. С. А. Ошерова. – М., 1977/(в пер.).
5. Вступ до філософії: навч. Посібник. / За ред. Нікітіна Л.М. – Донецьк. – 2003.
6. Бралатан В. П., Гуцаленко Л. В., Здирко Н. Г. Професійна етика: Навч. посібник. – К.:Центр учбової літератури, 2011. – 252 с.
7. Weil, Vivian (2008 р.). Professional ethics (Професійна етика). Доступно за посиланням: http://ethics.iit.edu/teaching/professional-ethics.
8. Філіппова Л. Я., Зеленецький В. С. Компьютерня етика. Морально-етичні і правові норми для користувачів компютерних мереж: Навч. посібн. – Харьків: Вид-во «Кроссроуд», 2006. – 209 с.
9. Ломачинська І.М., Рихліцька О.Д., Барна Н.В. Основи корпоративної культури.// Навч. посібник. – К.: 2011., – 480 с
10. Прикладна етика. Навч. посібник / За наук. ред. Панченко В.І.. – К.: «Центр учбової літератури», 2012. – Розділ 1. – С. 7-40.
11. Етика: Навч. посіб. / За ред. проф. В. О. Лозового. – К., 2004.
12. Чхеайло І.І., Чхеайло А.А. Інформаційна етика як моральна регуляція сучасного суспільства // Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія: Філософія, філософія права, політологія, соціологія. 2015. №3 (26). URL: https://cyberleninka.ru/article/n/informatsiyna-etika-yak-moralna-regulyatsiya-suchasnogo-suspilstva (дата звернення: 06.02.2023).
13. Коляденко В. Поняття «інформаційне суспільство» у класичних і сучасних концепціях. / В. Коляденко //Український науковий журнал «Освіта регіону» № 2, 2013. С. – 101-105.
14. Миролюбченко Г. А. Інформаційна етика в просторі сучасних комунікативних процесів (філософсько-етичний аналіз), Автореферат дисертації на здобуття наукового ступеня кандидата філософських наук – Київ, Київський національний університет імені Тараса Шевченка, 2011.

15. A. V. Preisig, H. Rösch, Ch. Stückelberger, Ethical Dilemasin the Information Society. Code of Ethics for Librerians and Archivists, Geneva, Globethics.net, 2014. – 220p. ISBN978-2-88931-023-4 (online version)https://www.ifla.org/wp-content/uploads/2019/05/assets/faife/publications/misc/ethical-dilemmas-in-the-information-society.pdf
16. Журналістська етика: Посібник для підготовки до державного іспиту / Авт. кол. - За ред. В. П. Мостового та В. В. Різуна. – Київ: ТзОВ «ЗН УА», 2014. – 224 с.
17. Кузнецова О.Д. Професійна етика журналістів: Посібник: 2-ге вид., перероб. І допов. – Львів: ПАІС, 2007. – 246 с.
18. Баева Л. В. Віртуальна комунікація: особливості і етичні принципи. Філософскі науки. 2015. № 10. С. 94-110.
19. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : Розпорядження Кабінету Міністрів України // Офіційний вісник України . – 2013. – № 44. – Ст. 1581.
20. Філіпова Л. Я., Зеленецький В. С. Комп'ютерна этика. Морально-етичні та правові норми для користувачів комп'ютерних мереж: Навч. посібн. – Харків: Вид-во «Кроссроуд», 2006. – 209 с.
21. Johnson Deborah G. Computer Ethics / 2nd ed. New Jersey: Prentice-Hall, Inc. Upper Saddle River, 1994. 181 p.
22. Хочь І. Проблеми формування інформаційної культури українського суспільства // Науковий вісник Ужгородського університету. Серія: Політологія, Соціологія, Філософія. 2010. Вип. 14. С. 250-253.
23. Про освіту. Закон України. Відомості Верховної Ради (ВВР), 2017, № 38-39, ст.380 – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/go/2145-19.
24. Про національну доктрину розвитку освіти. Затверджено Указом Президента України від 17 квітня 2002 року № 347/2002. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/go/347/2002.
25. Васянович Г.П. Педагогічна етика. Навчально-методичний посібник. – Л.: Просвіта, 2004. - 344 с.
26. Про наукову і науково-технічну діяльність. Закон України. Сайт Верховної Ради України. - [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/1977-12.

27. Академічна доброчесність як основа сталого розвитку університета / Міжнарод. благод. фонд « Міжнарод. фонд дослідж. освіт. політики», за заг. ред. Т. В. Філіпова, А. Є. Артюхова. – К.: Таксон, 2016. – 234 с.
28. Науковець А., Находкін М. Проблеми сучасності і мораль науковця // Вісник національної академії наук України. Загальнонауковий та громадсько-політичний журнал. – 2006. – №5. - [Електронний ресурс]. – Режим доступу http://www.nbuv.gov.ua/portal/all/herald/2006-05/a1-5.pdf .
29. Ліпкан В.А. Правові засади розвитку інформаційного суспільства в Україні : [монографія] / В. А. Ліпкан, І. М. Сопілко, В. О. Кір'ян / за заг. ред. В. А. Ліпкана. – К. : ФОП О. С. Ліпкан, 2015. – 664 с.
30. Про основні засади забезпечення кібербезпеки України. Закон України. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/go/2163-19.
31. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". Указ Президента України від 26 серпня 2021 року №447/2021.
32. Brey P. (2007). Ethical aspects of information security and privacy. In: Security, privacy, and trust in modern data management, data-centric systems and applications. Springer, Berlin/Heidelberg, pp 21–36. http://link.springer.com/content/pdf/10.1007/978-3-540-69861-6.pdf#page=36.
33. Markus Christen, Bert Gordijn, Michele Loi. The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology ISBN 978-3-030-29052-8 ISBN 978-3-030-29053-5 (eBook) https://doi.org/10.1007/978-3-030-29053-5.
34. Yaghmaei E, Van de Poel I, Christen M (2017) Canvas white paper 1 – cybersecurity and ethics, SSRN scholarly paper ID 3091909. Social Science Research Network, Rochester. https:// DOI:10.2139/ssrn.3091909.
35. Хартія основних прав Європейського Союзу [Архівовано 29 березня 2017 у Wayback Machine.] // Юридична енциклопедія : [у 6 т.] / ред. кол.: Ю. С. Шемшученко (відп. ред.) [та ін.]. – К. : Українська енциклопедія ім. М. П. Бажана, 2004. – Т. 6 : Т – Я. – 768 с.
36. Dittrich D, Bailey M, Dietrich S (2011) Building an active computer security ethics community. IEEE Secur Priv 9(4):32–40.
37. Andreas G. Scherer, Guido Palazzo and Dorothée Baumann. Corporate Ethics and Corporate Governance. Year: 2007, Page 309. DOI: 10.1007/978-3-540-70818-6_21

38. Лой, М., Крістен, М. (2020). Етичні рамки кібербезпеки. В: Крістен, М., Гордійн, Б., Лой, М. (ред.) Етика кібербезпеки. Міжнародна бібліотека етики, права та технологій, том 21. Спрінгер, Чам. https://doi.org/10.1007/978-3-030-29053-5_4.
39. Про основні засади забезпечення кібербезпеки України. Закон України. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403. [Електронний ресурс]. Режим доступу - https://zakon.rada.gov.ua/laws/show/2163-19.
40. Peleshchyshyn, A.. (2019). The Concepts of Philosophy of Information by Luciano Floridi. Visnyk of Kharkiv State Academy of Culture. https://doi.org/10.31516/2410-5333.055.02.
41. Kenneally, Erin E. and Dittrich, David, The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research (August 3, 2012). Available at SSRN: https://ssrn.com/abstract=2445102 or http://dx.doi.org/10.2139/ssrn.2445102.
42. Левін Р. Я. Інформована згода: деякі виклики загальній дійсності західної моделі //Право, медицина та охорона здоров'я. – 1991. – Т. 19. – No 3-4. – С. 207-213.
43. Дхай А. Еволюція дослідницької етики: від Нюрнберга до Гельсінкі //Південноафриканський медичний журнал. – 2014. – Т. 104. – No 3. – С. 178-180.
44. Всесвітня медична асоціація та ін Декларація Всесвітньої медичної асоціації Гельсінкі: етичні принципи медичних досліджень за участю людських суб'єктів //Jama. – 2013. – Т. 310. – No 20. – С. 2191-2194.
45. Бернетт С., Фемстер Н. Encore: Полегшене вимірювання веб-цензури за допомогою запитів перехресного походження //Матеріали конференції ACM 2015 року про спеціальну групу інтересів з передачі даних. – 2015. – С. 653-667. doi: 10.1145/2785956.2787485.
46. Макніш К. Конфіденційність у дослідницькій етиці //Довідник дослідницької етики та наукової доброчесності. – 2020. – С. 233-249.
47. Резнік Д. Б., Фінн П. Р. Етика та фішингові експерименти //Наука та інженерна етика. – 2018. – Т. 24. – С. 1241-1252. Doi: https://doi.org/10.1007/s11948-017-9952-9.
48. Levy, Steven. Hackers: Heroes of the Computer Revolution (updated edition). Penguin, 2001. ISBN 0-14-100051-1.

49. Norris P. AVirtuous Circle. Political Communication in Postindustril Societies. – L. – 2001.
50. Weinberg, Gerald M. The psychology of computer programming (вид. Silver anniversary). New York 2001, NY: Dorset House Publ. ISBN 978-0-932633-42-2.
51. Pekka Himanen/ The Hacker Ethic and the Spirit of the Information Age/ Edition in Russian. AST Publishers, 2019.
52. Карпчук Н.П. Міжнародна інформація та суспільні комунікації : навч. посіб. для студ. закл. вищ. освіти / Н. П. Карпчук. – Луцьк ; 2018. – 514 с.
53. Савченко В.А., Шаповаленко О.Д. Основні напрямки застосування технологій штучного інтелекту у кібербепеці. /Сучасний захист інформації №4(44), 2020. С. 6-11. DOI: 10.31673/2409-7292.2020.040611.
54. M. Vielberth, F. Bohm, I. Fichtinger and G. Pernul, "Security operations center: A systematic study and open challenges", IEEE Access, vol. 8, pp. 227756-227779, 2020. DOI: 10.1109/ACCESS.2023.3255101
55. Когут Ю. І. Корпоративна безпека : практичний посібник / Ю. І. Когут. – Київ: Консалтингова компанія Сідкон, 2021. – 460 с.
56. Задихайло Д.В., Кібенко О.Р., Назарова Г.В. Корпоративне управління. Навчальний посібник. – Х .: Еспада, 2003. – 688 с.
57. Кубко В.П. Процес створення корпоративних кодексів. /Праці Одеського політехнічного університету, 2008, вип. 1(29). С. 317-314.
58. Нідзієва В.А. Корпоративний кодекс як інструмент управління організаційною культурою загальноосвітніх навчальних закладів [Електронний ресурс] – Режим доступу: URL: http://nbuv.gov.ua/UJRN/Otros_2015_7_10.
59. Фукуяма Ф. Довіра: соціальні чесноти та шлях до процвітання. [Електронний ресурс] – Режим доступу: https://doi.org/10.2307/20047503.
60. Кукура С.П. Теорія корпоративного управління. М.: Економіка, 2004. 478 с.
61. Про банк. «ПриватБанк», 2014. [Електронний ресурс] – Режим доступу: URL: https://privatbank.ua/about.
62. Кодекс корпоративної етики. НАК «Нафтогаз», 2013. [Електронний ресурс] – Режим доступу: URL: http://www.naftogaz.com/files/HR/Naftogaz–Code–Ethics.pdf.
63. КСВ. 1+1 Медіа. ТРК «Студія 1+1», 2017. [Електронний ресурс] – Режим доступу: URL: https://media.1plus1.ua/ua/csr/employees.

64. Управління конфліктами для потреб публічної служби: посібник і методичні рекомендації / Калениченко Т., Кисельова Т., Копіна А., Корабльова О., Проценко Д., за заг. ред. Д. Проценко. – Київ: Ваіте, 2021. – 224 с.
65. 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.
66. Савченко В. А Модель інформаційного стримування між державами на основі теорії рефлексивних ігор / Савченко В. А., Дзюба Т. М. //Сучасний захист інформації №2(42), 2020. С. 6-18. DOI: 10.31673/2409-7292.2020.020618.
67. Шмітт, Майкл Н., Класифікація кіберконфліктів (5 вересня 2012 р.). 17 Журнал права про конфлікти та безпеку 245 (2012), доступний у SSRN: https://ssrn.com/abstract=2184831.
68. Bansal, Gaurav; Hodorff, Kayla; and Marshall, Kyle, "Moral Beliefs and Organizational Information Security Policy Compliance: The Role of Gender" (2016). MWAIS 2016 Proceedings. 11. 1-6 pp. http://aisel.aisnet.org/mwais2016/11.
69. Siponen, Mikko & Vance, Anthony. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Quarterly: Management Information Systems. 34. 487-502. https://doi.org/10.2307/25750688.
70. Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. 2014. "Variables influencing information security policy compliance," Information Management & Computer Security (22:1), pp 42-75. https://doi.org/10.1108/IMCS-08-2012-0045.
71. Kadenko, Sergii & Tsyganok, Vitaliy & Andriichuk, Oleh & Karabchuk, A. Аналіз інструментарію підтримки прийняття рішень у контексті вирішення задач стратегічного планування. Реєстрація, зберігання і обробка даних. №22(2). 2020. с. 77-91. DOI:10.35681/1560-9189.2020.22.2.211281.
72. Платформа для підвищення кібербезпекикритично важливих інфраструктур. Національний інститут стандартів та технологій. 2018 р. Ця публікація доступна безкоштовно за адресою: https://doi.org/10.6028/NIST.CSWP.04162018uk.

Інформаційні електронні ресурси

1. Електронна бібліотека ДУТ: https://www.dut.edu.ua/ua/lib/1/category/2122
2. Електронні матеріали в MOODLE : Курс: Корпоративна та професійна етика в кібербезпеці (dut.edu.ua)
3. Інтернет-ресурси:

- http://www.nbuv.gov.ua/ - сайт Національної бібліотеки України
- http://www.scientific-library.net – Електронна бібліотека науково-технічної літератури
- https://www.unodc.org/documents/e4j/IntegrityEthics/E4J_Integrity_and_Ethics_Module_14_final_UKR.pdf – професійна етика
- https://kneu.edu.ua/ua/science_kneu/ndi/prikl_etiki/ - сайт інституту прикладної та професійної етики

АЛФАВІТНИЙ ПОКАЖЧИК

ДОДАТКИ

Додаток А

ЗРАЗОК КОДЕКСУ ПРОФЕСІЙНОЇ ЕТИКИ

КОДЕКС ПРОФЕСІЙНОЇ ЕТИКИ
НАУКОВО-ПЕДАГОГІЧНОГО ПРАЦІВНИКА
ОНАЗ ім. О. С. ПОПОВА

ПРЕАМБУЛА

Кодекс Професійної етики науково-педагогічного працівника Одеської національної академії зв'язку ім. О.С. Попова (далі – Кодекс) – це правила його поведінки в академічному середовищі.

Метою Кодексу є формування в академії системи демократичних заємовідносин з високим ступенем етичної гідності між студентами, науково-педагогічними працівниками, співробітниками й адміністрацією та розвиток корпоративної культури академічного співтовариства.

Науково-педагогічний працівник Одеської національної академії зв'язку ім. О. С. Попова

- усвідомлюючи себе громадянином України, шануючи мову, історію та культуру українського народу, працюючи для добробуту та процвітання держави;
- розуміючи свою відповідальність за реалізацію місії академії – зміцнення освітньо-професійного та наукового потенціалу держави шляхом високоякісної підготовки фахівців для підприємств, організацій та установ усіх форм власності галузі зв'язку та інформатизації та інших галузей економіки, конкурентоспроможних на світовому ринку праці і готових до плідної професійної діяльності;
- вважаючи своїм обов'язком безпосередню участь у формуванні іміджу та підвищенні престижу Одеської національної академії зв'язку ім. О.С. Попова – відомого центру підготовки національної еліти;
- пропагуючи ідеї розвитку інформаційного суспільства, розповсюдження наукових знань в цій області;
- прагнучи до формування системи демократичних взаємовідносин між студентами, науково- педагогічними працівниками, співробітниками й адміністрацією та розвитку корпоративної культури академічного співтовариства, схвалює цей Кодекс і зобов'язується неухильно його дотримуватись.

ОСНОВНІ ПОЛОЖЕННЯ

Стаття 1

Науково-педагогічний працівник у своїй діяльності дотримується Конституції України, чинного законодавства України, Статуту, Правил внутрішнього розпорядку й інших нормативних актів академії.

Стаття 2

Науково-педагогічний працівник шанобливо ставиться до Гімну, Прапора і Герба України та Гімну та Прапора академії як важливих атрибутів, які сприяють вихованню почуття любові до України, рідної академії, корпоративної єдності та єднання.

Стаття 3

Науково-педагогічний працівник бере безпосередню та активну участь у формуванні та розвитку в академії системи менеджменту якості освіти.

Стаття 4

Науково-педагогічний працівник дбає про підтримку високої академічної культури, атмосфери довіри і взаємної поваги в академічному співтоваристві.

Стаття 5

Науково-педагогічний працівник сумлінно ставиться до проведення навчального процесу й усіх форм контролю набутих студентами знань, вмінь та навичок (компетенції), вважаючи при цьому неприпустимою нечесність та недбалість.

Стаття 6

Науково-педагогічний працівник має брати активну участь у проведенні наукових досліджень, вважаючи їх основою розвитку суспільства та невід'ємною складовою існування вищої школи.

Стаття 7

Науково-педагогічний працівник дбає про постійне підвищення своєї професійної кваліфікації, застосовує у своїй навчально-педагогічній діяльності сучасні освітні методи та технології.

Стаття 8

Науково-педагогічний працівник здійснює свою діяльність на засадах принципів незалежності від політичних партій та релігійних організацій.

Стаття 9

Науково-педагогічний працівник дотримується демократичної політичної культури (демократичних норм, цінностей, традицій) у своїй діяльності, зокрема, дотримує закони України, які не припускають залучення студентів до політичних акцій під час навчально-виховного процесу і не пропагує свої політичні погляди та переконання у навчальному закладі.

Стаття 10

Науково-педагогічний працівник дотримує закони України, які не припускають залучення студентів в релігійних акціях під час навчально-виховного процесу і не пропагує свої релігійні погляди та переконання у навчальному закладі

Стаття 11

Науково-педагогічний працівник виявляє толерантність та повагу до звичаїв і традицій студентів, колег та співробітників усіх національностей, поважає культурні та інші особливості різних етнічних та соціальних груп і конфесій.

Стаття 12

Науково-педагогічний працівник підтримує конструктивну діяльність, спрямовану на зміцнення системи студентського самоврядування, розвиток студентської творчої активності (освітньої, наукової, спортивної, художньої тощо), підвищення корпоративної культури та іміджу академії.

Стаття 13

Науково-педагогічний працівник не допускає порушення академічних норм, зокрема:

- порушення вимог нормативно-правових документів, що стосуються організації, забезпечення та проведення навчального процесу;
- невиконання індивідуального робочого плану;
- провадження навчального процесу без його повного організаційного та науково-методичного забезпечення;
- запізнення на навчальні заняття, їх пропуск без поважних причин, неповне та неефективне використання запланованого навчального часу;
- установлення зі студентами відносин, не передбачених чинним законодавством України, Статутом, Правилами внутрішнього розпорядку та іншими нормативними актами академії;
- здійснення дій, пов'язаних з впливом на хід навчального процесу будь-яких особистих, майнових, фінансових та інших інтересів;
- необ'єктивне проведення поточного, модульного та семестрового контролю;
- некоректне, нешанобливе ставлення до студентів, колег, інших співробітників;
- використання родинних або службових зв'язків в особистих інтересах;
- пасивність у своїй діяльності на кафедрі та академії взагалі, розглядаючи ці порушення академічних норм як несумісні з його діяльністю, спрямованою на забезпечення здобуття студентами якісної та конкурентоспроможної вищої освіти, гідної майбутньої інтелектуальної еліти України.

Стаття 14

Науково-педагогічний працівник дбайливо ставиться до літературних фондів бібліотеки, документів кафедр та академії, інших інформаційних ресурсів (на електронних та неелектронних носіях).

Стаття 15

Науково-педагогічний працівник дбає про збереження майна та раціональне використання енергоносіїв академії, протидіє проявам вандалізму в приміщеннях та на її території.

Стаття 16

Науково-педагогічний працівник не допускає поведінки, здатної завдати шкоди репутації та іміджу академії.

Стаття 17

Науково-педагогічний працівник не повинен бути байдужим до порушень суспільних норм з боку студентів чи співробітників і повинен вказати на неприпустимість такої поведінки порушникові.

Стаття 18

Науково-педагогічний працівник дотримується ділового стилю в одязі, дбає про охайність зовнішнього вигляду (без підкресленої екстравагантності).

Стаття 19

Науково-педагогічний працівник протидіє порушенням Кодексу з боку студентів, колег та співробітників і повинен сповістити про порушення адміністрацію академії.

Стаття 20

До науково-педагогічного працівника, який порушив положення Кодексу, застосовуються заходи впливу відповідно до чинного законодавства України, Статуту, Правил внутрішнього розпорядку та інших нормативних актів академії.

Стаття 21

Визнання науково-педагогічним працівником положень Кодексу і обов’язок їх виконання в процесі своєї професійної діяльності засвідчується його особистим підписом під час прийому на роботу до академії.

Додаток Б

Кодекс корпоративної етики H-X Technologies (системи безпеки)

1. Корпоративна етика – це норми поведінки членів нашої команди, засновані, перш за все, на наших цінностях, корпоративній культурі, бізнес-етиці, а також на правах людини.

2. Принципи корпоративної етики компанії “H-X Technologies” є загальними та обов’язковими для всіх членів команди, незалежно від посади. Це відноситься також до будь-яких інших осіб, які діють від імені компанії.

3. Наші фахівці не просто поділяють цінності компанії та керуються у своєму житті прийнятими нормами поведінки, а й вносять свій внесок у подальше вдосконалення нашої корпоративної культури.

4. Ми цінуємо атмосферу доброзичливості, дружності, довіри та взаємної підтримки. Висока якість наших сервісів і продуктів пов’язана зі сприятливим психологічним кліматом у компанії.

5. Ми прагнемо створювати умови, необхідні для успішного виконання роботи, відкритого та своєчасного спілкування, здорового робочого клімату, професійного та особистісного зростання, а також самореалізації.

6. Ми поважаємо гідність і особистість кожного. Залякування, погрози, образи, приниження та прояви нетерпимості неприпустимі в нашій команді.

7. Фахівці компанії “H-X Technologies” працюють чесно та сумлінно, несуть відповідальність за результати своєї роботи та дотримуються трудової дисципліни.

8. Ми дотримуємося політики рівних можливостей – успіх кожного залежить тільки від його знань, технічних і соціальних навичок, досвіду, а також від результатів роботи.

9. Компанія “H-X Technologies” діє відповідно до загальноприйнятих міжнародних норм захисту прав людини. У нас немає дискримінації за ознаками статі, віку, кольору шкіри, національності, раси чи релігії.

10. Компанія “H-X Technologies” прагне робити внесок в охорону навколишнього середовища планети, а також здоров’я співробітників і всіх людей.

11. Ми дорожимо своєю репутацією, дотримуємося законів, етичних норм і правил справедливого ведення бізнесу. Ми суворо виконуємо свої зобов'язання перед замовниками, партнерами, фахівцями та колегами.

12. Кожен фахівець компанії підписує зобов'язання про дотримання конфіденційності, яке залишається в силі навіть після припинення співпраці з компанією.

13. Ми дотримуємося клієнтоорієнтованого підходу у всіх своїх проектах і завданнях – як зовнішніх, так і внутрішніх.

14. В основі наших відносин із замовниками лежить повага та розуміння. Ми прагнемо надати замовникові свої послуги та продукти найвищої якості та в заздалегідь узгоджені терміни. Основними чинниками нашої конкурентоспроможності є висока якість і справедливі ціни.

15. Компанія "H-X Technologies" підтримує справедливу та відкриту конкуренцію. Ми не порушуємо антимонопольні закони та закони з питань конкуренції. Ми не використовуємо заборонені методи конкуренції.

16. Бухгалтерський облік компанії «H-X Technologies» гарантує правильне здійснення всіх бухгалтерських операцій відповідно до законодавства та загальноприйнятих бухгалтерських стандартів.

17. Компанія "H-X Technologies" проти корупції. Ми не пропонуємо та не приймаємо подарунки або винагороди з метою одержання неправомірної вигоди.

18. Компанія "H-X Technologies" проти відмивання грошей. Ми вживаємо заходів щодо боротьби з фінансовими операціями з метою відмивання грошей.

19. Компанія "H-X Technologies" не підтримує будь-які політичні партії та течії, а також будь-які збройні конфлікти, незалежно від їхніх цілей.

20. Кожен фахівець нашої команди несе персональну відповідальність за дотримання всіх перерахованих вище принципів, правил і обмежень, а також релевантних законів, норм і стандартів.

Додаток В

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

СХВАЛЕНО
Постанова загальних зборів
НАН України 15.04.2009 N 2

Етичний кодекс ученого України

Передмова

Метою Етичного кодексу вченого України (надалі Кодекс) є формулювання загальних етичних принципів, яких кожен з науковців і викладачів має дотримуватися у своїй роботі. Кодекс регулює відносини науковців між собою та із суспільством. Він установлює основні засади для оцінки вченими своєї власної роботи та діяльності колег під моральним кутом. Закріплені тут принципи мають слугувати основою для етичної підготовки молодих науковців.

Основним завданням Кодексу є надання пріоритету моральним вимірам науки та соціальній відповідальності спільноти вчених і кожного вченого зокрема. Проблема особистої відповідальності вченого набула важливого значення тому, що суспільні інститути часом не встигають за стрімкими темпами розвитку науки і технологій.

В усьому світі етичні кодекси базуються на розумінні того, що належна практика у сфері науки сприяє довірі в середовищі наукового співтовариства та між ним і суспільством, що є необхідним для розвитку науки. Вчені повинні бути впевненими в надійності результатів роботи своїх колег. У свою чергу, суспільство має бути впевненим у чесності науковців та достовірності результатів їхніх досліджень. На жаль, останнім часом така довіра похитнулася у зв'язку з тим, що в багатьох країнах спостерігалися серйозні порушення етики, які підірвали авторитет науки та довіру суспільства до вчених. Щоб запобігти такому розвиткові подій в Україні, всі науковці мають усвідомлювати важливість високоетичної поведінки та свою відповідальність за формування громадської думки щодо науки.

1. Загальні принципи

1.1. Етика науки базується на основоположних цінностях, нормах та принципах і визначає моральну поведінку вченого, його відповідальність перед суспільством.

1.2. У своїй роботі вчений має керуватися визнаними стандартами практики, загальні положення яких сформульовано у цьому Кодексі.

1.3. Учений повинен усвідомлювати, що ефективність науки оцінює суспільство.

1.4. Учений несе моральну відповідальність за наслідки своєї діяльності, що можуть впливати на розвиток людства або природи. Вчений повинен протидіяти отриманню результатів, що суперечать принципам гуманізму, шляхом.

- відмови у співпраці;

- попередження суспільства про можливі негативні наслідки використання досягнень науки в антигуманному напрямку;

- інформування громадськості, зокрема наукового співтовариства, щодо можливих негативних наслідків застосування наукових досягнень і необхідності їх попередження.

1.5. Учений зобов'язаний протидіяти конформізму в науковому співтоваристві, брати активну участь у процесах атестації наукових кадрів, протидіяти присудженню наукових ступенів і звань за роботи, які не відповідають сучасним досягненням світової науки або виконані з порушенням норм етики, зокрема рішуче викривати факти плагіату й інших форм порушень авторського права.

1.6. Учений має активно протидіяти псевдонауці, виступати проти розповсюдження в суспільстві її поглядів і рекомендацій.

1.7. Вчений має спрямовувати свої зусилля на подальше застосування отриманих знань задля блага людства, збереження навколишнього середовища та найекономічнішого використання природних ресурсів. Визнаючи суспільні отреби та обмеженість природних ресурсів, чений повинен активно протидіяти проведенню необґрунтованих досліджень.

1.8. Свобода в науці - це в першу чергу свобода вибору наукових напрямів дослідження, концепцій, гіпотез, парадигм, проблем і методів їхнього вирішення, й понад усе, свобода думки та слова. Свобода в науковій творчості в своїй основі повинна мати високий професіоналізм. Учений має захищати

свободу наукової думки, засуджувати цензуру щодо наукової творчості та будь-які намагання монополізувати ті чи інші напрями науки.

1.9. Учений несе відповідальність за виникнення небезпеки для окремої людини, суспільства, економіки або шкоди для природи, які може заподіяти застосування неперевірених нових наукових знань.

1.10. Учений не чинить дій, які можуть завдати шкоду професійній репутації іншого вченого. Проте, за наявності неспростовних доказів неетичної поведінки чи непрофесійних дій ученого, наукове співтовариство має у відкритій неупередженій дискусії дати їм відповідну оцінку.

1.11. Учений має докладати зусиль до підготовки та розвитку наукової молоді - інтелігентів, чесних і самовідданих патріотів. Тому виховання наукової зміни не повинно обмежуватися ільки наданням технічних навичок, необхідних для проведення дослідження. Підготовка має включати основні етичні стандарти та норми науки. Наукові співробітники та викладачі мають слугувати взірцем моральності для молодих вчених щодо ставлення до науки та до авторських прав.

2. Наукові дослідження

2.1. Учений має дотримуватися найвищих професійних стандартів планування та проведення наукових досліджень на основі глибоких знань про доробок світової науки у певній галузі.

2.2. Учений зобов'язаний вишукувати найприйнятніші з огляду на адекватність та економічну виправданість шляхи вирішення досліджуваної проблеми. Висновки завершеного дослідження вчений зобов'язаний викладати об'єктивно, незважаючи на очікування замовника.

2.3. Учений має забезпечувати бездоганну чесність і прозорість на всіх стадіях наукового дослідження та вважати неприпустимим прояви шахрайства, зокрема фабрикування та фальшування даних, піратства і плагіату. Неприпустимим є намагання керівних осіб упереджено впливати на характер отримуваних в дослідженні даних і висновків. Учений служить лише об'єктивній істині.

2.4. Учений має пам'ятати, що наукове дослідження - це процес отримання нового знання. Він має прагнути до належної ерудиції і компетентності, за яких можливий критичний аналіз найсучасніших наукових знань.

2.5. Учений має забезпечувати необхідний захист інтелектуальної власності.

2.6. Вчений має сприяти якнайповнішому використанню результатів своєї праці в інтересах суспільства та з метою охорони довкілля.

2.7. Наукові дослідження жодним чином не повинні ображати гідність або йти всупереч правам людини. У медико-біологічних дослідженнях слід керуватися принципами біоетики.

2.8. Наукове дослідження має проводитися таким чином, щоб не спричиняти шкоди навколишньому середовищу. Якщо такого пошкодження неможливо уникнути, вплив людини повинен бути зведений до мінімуму, а середовище після завершення дослідження відновлене до його первинного стану.

3. Учений як автор

3.1. Основною мотивацією діяльності вченого має бути прагнення до пізнання та бажання збагатити науку новими знаннями. При цьому найвищою нагородою вченого є досягнення істини та визнання наукового співтовариства. Вчений має право та обов'язок захищати свій науковий пріоритет. Разом з тим, публікація неточних і непереконливих наукових результатів, а також публікація в ненаукових виданнях з метою досягнення пріоритету, неприпустимі.

3.2. Учений визнає міжнародні та національні правові норми щодо авторських прав. Він може використовувати інформацію з будь-яких публікацій за умови, що вказує джерело та проводить чітку межу між власними даними та здобутками інших. Запозичення для власних публікацій будь-яких фотографій, рисунків, таблиць, схем тощо потребує, згідно з видавничими правилами, дозволу автора або видавництва.

3.3. При публікації результатів дослідження, що проводилося групою вчених, всі, хто брав творчу участь у роботі, мають бути зазначеними як автори; у разі необхідності може бути зазначено їхній особистий внесок. Тільки реальний творчий внесок у наукову роботу може слугувати критерієм авторства. Поступатися авторством на наукову роботу іншій особі, приймати авторство або співавторство та, особливо, вимагати його є неприпустимим.

3.4. Учений не повинен повторювати свої наукові публікації з метою підвищення їх кількості. Якщо для пропаганди наукових досягнень доцільна публікація однієї і тієї ж роботи в різних журналах, редактори останніх повинні бути поінформовані про факт публікації в інших виданнях.

3.5. Учений повинен бути об'єктивним в оцінці власних досягнень. Преса, радіо та телебачення можуть бути використані для пропаганди наукових досягнень, але не власної особи. При публікації роботи вчений

підпорядковується вимогам видавця, але бажано, щоб наукові ступені та звання автора не були вказані. Така інформація може бути подана у примітці.

4. Учений як керівник

4.1. Для наукової праці вчений оточує себе співробітниками тільки на основі неупередженої оцінки їхніх інтелектуальних, етичних і персональних рис. Учений повинен протидіяти всім проявам протекціонізму, корупції і дискримінації.

4.2. Учений будує взаємини зі співробітниками на принципах справедливості, виявляє доброзичливість і підтримку своїм учням та оцінює кожного з них об'єктивно. Як керівник він має сприяти службовому зростанню підпорядкованих йому співробітників відповідно до їхньої кваліфікації і ставлення до праці.

4.3. Учений не перекладає на своїх співробітників виконання завдань, які він повинен виконувати сам.

4.4. Учений-керівник зобов'язаний обґрунтовувати, але не нав'язувати членам свого колективу своє наукове бачення проблеми.

4.5. Учений повинен докладати всіх зусиль для створення належної творчої атмосфери в колективі.

5. Учений як викладач

5.1. Учений має з повагою ставитися до своїх учнів і до їхнього вільного й критичного мислення.

5.2. Учений у своїй викладацькій роботі повинен не лише доносити до аудиторії достовірну наукову інформацію, але й сприяти становленню громадянської позиції молодого покоління.

5.3. Учений не повинен перешкоджати спілкуванню своїх учнів з іншими вченими та науковими інституціями. Він поважає їх право на вільне об'єднання, самоврядування та членство в колегіальних академічних організаціях, прислухається до думки студентського співтовариства щодо форми та методів навчання.

5.4. Учений повинен проводити заняття в цікавій формі, прийнятній для широкого кола учнів. Він має переконатися в належному забезпеченні лабораторій та бібліотек, заняття проводити суворо відповідно до розкладу. Зміст лекцій повинен відображати сучасні досягнення світової науки і не супроводжуватися тиском упередженої думки.

5.5. Учений має об'єктивно ставитися до учнів, утримуючись від неетичних форм оцінок.

5.6. Учений має усвідомлювати, що він повинен бути взірцем найвищої інтелігентності, в якій відображаються традиції визнаних українських і світових наукових шкіл.

5.7. Учений приділяє особливу увагу обдарованим студентам і залучає їх до наукової праці. Він має виховувати у своїх учнів почуття відповідальності за наукову діяльність.

5.8. Учений не розголошує інформацію особистого характеру щодо своїх учнів.

5.9. Учений не приймає жодної оплати чи іншого доходу від своїх студентів. Не дозволяється проведення індивідуальних чи групових занять або консультацій, безпосередньо оплачуваних студентами.

6. Учений як консультант чи експерт

6.1. Учений має виступати експертом тільки у сфері своєї компетенції відповідно до своїх знань і досвіду.

6.2. Учений має дотримуватися принципу рівності при проведенні експертного розгляду. Будь-яка дискримінація на підставі статі, раси, політичних поглядів чи культурної та соціальної приналежності є несумісною з цим принципом.

6.3. Учений висловлює свою думку про роботу та наукові досягнення колег чесно, чітко та неупереджено. Як вишукано ввічливі та прихильні, так і упереджено негативні висловлювання не припустимі. Підготовка об'єктивного критичного висновку повинна розглядатися як обов'язок, від виконання якого вчений не має права ухилятися.

6.4. Учений несе персональну відповідальність за чесну й об'єктивну оцінку кандидатських і докторських дисертацій. Виступаючи в ролі опонента при захисті дисертаційних робіт, учений має бути неупередженим.

6.5. Під час обговорення, полеміки та висловлювання критичних зауважень учений повинен дотримуватися принципів рівноправності, фактичної обґрунтованості та достовірності. Принцип рівноправності гарантує рівні права всім учасникам дискусії або полеміки незалежно від наукових ступенів і звань. Принцип фактичної обґрунтованості виключає необ'єктивну критику. Принцип достовірності забороняє будь-які перекручування з метою приниження або дискредитації.

6.6. При проведенні експертного розгляду вчений має дотримуватися принципу конфіденційності.

6.7. У ході експертного розгляду вчений має зберігати незалежність і не піддаватися тиску при підготовці та виголошенні висновків.

6.8. Обираючи кандидатів для проведення дослідження або на інші наукові посади, вчений як експерт має об'єктивно оцінювати претендентів. Він не повинен надавати перевагу своїм учням, представникам своєї наукової школи тощо. При конфлікті інтересів учений повинен ставити загальні інтереси вище, ніж інтереси замовників дослідження.

7. Учений як громадянин

7.1. Учений має присвятити себе пошукові нових знань та їх застосуванню на благо суспільству та для збереження природи. Інформація, яка надається суспільству, має бути достовірною. Вчений протидіє поширенню неперевірених даних і необґрунтованих рекомендацій.

7.2. Учений сприяє розповсюдженню наукових знань і протидіє поширенню псевдонаукових теорій, хибних концепцій та уявлень.

7.3. Учений повинен оприлюднювати результати своїх досліджень не лише у спеціальних наукових виданнях, але й у науково-популярній формі, щоб зробити їх максимально доступними для широких верств суспільства.

7.4. Учений повинен брати активну участь у житті наукового співтовариства та у роботі колегіальних органів. При цьому він має діяти, насамперед, виходячи із загальних інтересів науки й тільки потім з інтересів особистих та своєї установи.

7.5. Учений не дозволяє використовувати авторитет науки чи свій власний авторитет у рекламних або пропагандистських цілях з корисливою метою.

7.6. Учений, що займає урядову чи адміністративну посаду, повинен дотримуватися етичних норм, прийнятих у науковому співтоваристві.

Додаток Г

Кодекс EthicsFIRST

Кодекс EthicsFIRST - це сукупність принципів, вкладених у підвищення етичності поведінки у технологічної промисловості.

1. Етичність - понад усе
   Перевіряючи інформацію та технології, ми беремо відповідальність за те, щоб використовувати їх етично та справедливо.
2. Рівність та справедливість
   Ми ставимо рівність та справедливість у центр нашої роботи та сприяємо створенню технологій, які допомагають вирішувати соціальні проблеми.
3. Відкритість та прозорість
   Ми відкриті та прозорі в нашій роботі та спілкуванні, щоб наші дії та прийняті рішення були зрозумілі та перевіряються.
4. Конфіденційність та захист даних
   Ми захищаємо конфіденційність та безпеку даних користувачів та гарантуємо, що вони використовуються лише відповідно до закону та згоди користувачів.
5. Соціальна відповідальність
   Ми беремо на себе соціальну відповідальність та створюємо технології, які допомагають вирішувати суспільні проблеми та покращують життя людей.
6. Стійкість та екологічна відповідальність
   Ми прагнемо стійкості та екологічної відповідальності в нашій роботі, щоб зменшити негативний вплив технологій на навколишнє середовище та зберегти його ресурси для майбутніх поколінь.
7. Навчання та розвиток
   Ми постійно навчаємось і розвиваємося, щоб бути в курсі новітніх технологій та етичних стандартів та застосовувати їх у своїй роботі.
8. Дотримання правил та законів
   Ми дотримуємось усіх застосовних правил і законів, пов'язаних з нашою роботою, і діємо відповідно до високих етичних стандартів.
9. Інклюзивність та різноманітність
   Ми заохочуємо інклюзивність та різноманітність у нашій роботі та в команді, щоб створювати технології, які враховують потреби всіх користувачів, незалежно від їхньої раси, статі, віку, національності, орієнтації та інших характеристик.
10. Неприскорений прогрес
    Ми дотримуємося принципу неприскореного прогресу, щоб технології розвивалися відповідно до етичних стандартів і не створювали небезпеки для людей та суспільства загалом.

11. Відповідальність за рішення
    Ми приймаємо відповідальність за наші рішення та дії, і готові відповідати за них перед суспільством та законом.
12. Відкритий діалог
    Ми заохочуємо відкритий діалог та обмін думками, щоб знайти найкращі рішення та досягти консенсусу в етичних питаннях.
13. Принцип запобігання шкоді
    Ми дотримуємося принципу запобігання шкоди та прагнемо мінімізувати можливий негативний вплив на технології на суспільство та довкілля.
14. Обов'язкове навчання та контроль
    Ми обов'язково проходимо навчання з етики та етичних стандартів і контролюємося, щоб гарантувати, що наші дії відповідають цим стандартам.
15. Постійне вдосконалення
    Ми прагнемо постійного вдосконалення та покращення нашої роботи, щоб забезпечити максимальну етичність і відповідність високим стандартам у нашій області.
16. Підтримка спільноти
    Ми підтримуємо спільноту та докладаємо зусиль для створення технологій, які враховують потреби та інтереси всіх людей у суспільстві.
17. Етичне лідерство
    Ми прагнемо етичного лідерства та підтримуємо наших колег та партнерів у їхніх зусиллях зі створення етичних технологій.
18. Принцип добровільності
    Ми дотримуємося принципу добровільності при отриманні даних користувачів та зобов'язуємося використовувати їх тільки з дозволу користувачів.
19. Створення безпечних технологій
    Ми зобов'язані створювати технології, які є безпечними та не порушують права користувачів.
20. Стриманість в рекламі
    Ми дотримуємося принципу стриманості в рекламі та не намагаємося впливати на користувачів неетичними методами.
21. Транспарентність та чесність
    Ми прагнемо до транспарентності та чесності в нашій роботі та відкритості перед користувачами.
22. Створення інновацій
    Ми прагнемо до створення інноваційних рішень, які не тільки сприятимуть розвитку технологій, але й відповідатимуть етичним принципам та стандартам.

Навчальне видання

ЛЕГОМІНОВА Світлана Володимирівна
ЩАВІНСЬКИЙ Юрій Віталійович
МУЖАНОВА Тетяна Михайлівна
ЯКИМЕНКО Юрій Михайлович
КАПЕЛЮШНА Тетяна Вікторівна
РАБЧУН Дмитро Ігорович

ПРОФЕСІЙНА ЕТИКА УПРАВЛІНСЬКОЇ ДІЯЛЬНОСТІ В КІБЕРБЕЗПЕЦІ

Навчально-методичний посібник

Надруковано у РВЦ Державного університету телекомунікацій
Формат 60х90/16. Папір друкарський
Наклад 100 прим. Зам. 50.

Свідоцтво суб'єкта видавничої справи ДК №6185 від 17.05.2018 р.

03110, м. Київ, вул. Соломянська, 7.
Тел. (044) 249-25-76