**УДК 340.12**

© 2015 р. **В.Б. Войчишин**
Чернівецький національний університет імені Юрія Федьковича, Чернівці

# АКТУАЛІЗАЦІЯ ОНТО-ГНОСЕОЛОГІЧНОЇ МОДЕЛІ КІБЕРНЕТИЧНОГО ЗЛОЧИНУ

Розкривається специфіка й особливості пізнавальних процесів, які мають місце в кібернетичному просторі є результатом пізнавальної діяльності суб'єкта та спрямовані на скоєння кібернетичних злочинів. Класифікація гносеологічних суб'єктів дає змогу детальніше зрозуміти, хто, за яких умов та для чого вчиняє кібернетичний злочин.

*Ключові слова:* пізнання, пізнавальний процес, гносеологічний суб'єкт, кібернетичний злочин, віртуальний простір, деструктивний запит, причина, мета, вина.

**Постановка проблеми.** Гносеологічна проблематика завжди викликала великий інтерес у сфері науки, адже пізнавальні процеси є необхідною умовою для розвитку та життєдіяльності суспільства. Будь-яке відкриття у галузі науки завжди зумовлене інтенсивними пізнавальними процесами, які здатні відкрити людству нові знання, або переосмислити вже набуті. Пізнавальна інтенсивність пронизує весь буттєвий устрій, задаючи темп і параметри розвитку соціально-правових процесів, не обійшовши стороною віртуальний простір. Останній створив підходящі умови для переходу правових феноменів до нового, раніше незвіданого середовища. Нововведення, окрім позитивних наслідків, призвели до появи негативних процесів, що не лише дестабілізували віртуальний простір, а й призвели до формування цілеспрямованих протиправних дій – кібернетичних злочинів.

**Мета статті.** Полягає у розкритті особливостей пізнавальних процесів у кібернетичному просторі, а також класифікації та визначенні основних гносеологічних суб'єктів, без яких унеможливлюється не лише скоєння кібернетичних злочинів, а й існування кібернетичного простору загалом. Проблемами пізнання у філософському вимірі у свій час займалися такі вчені: І. Кант, Г. Лейбніц, Р. Декарт, М. Хайдеггер, Е. Гуссерль, К. Свасьян та інші. У правознавстві гносеологічний напрям пов'язаний із такими науковцями: П. Рабінович, А. Козловський, С. Сливка, Н. Гураленко, Ю. Пермяков, В. Малахов, Ю. Закомлістов.

**Виклад основного матеріалу.** У зв'язку із досліджуваною проблематикою виникає запитання: Але на що ж опирається пізнання? Що є джерелом його внутрішньої енергії? Хто зумовлює пізнавальний процес та є його беззаперечним автором і творцем?

На думку вірменського феноменолога К.Свас'яна, пізнавальні процеси, перш за все, опираються на досвід і професійно засвоєний інструментарій понять і термінів, а також на мисленнєві традиції, характерні для даної епохи [1, с. 48]. Характер епохи знаходить своє відображення у розвитку та впровадженні різноманітних технологій та конструкторських рішень у сферу людської діяльності, що дають змогу людині по-іншому виконувати поставлені перед нею пізнавальні завдання. Відповідних гносеологічних змін зазнав також феномен злочину. Новітні технології створили новітнє середовище, яке дало життя кібернетичним злочинам, а також створили нові можливості й умови для пізнання. Продовжуючи думку вірменського феноменолога з приводу природи пізнавальних процесів, спробуємо застосувати вищесказане до специфіки кібернетичних злочинів. Досвід відіграє чи не найважливішу роль при підготовці та скоєнні кібернетичного злочину. Адже він є необхідною умовою у формуванні пізнавального процесу, оскільки розпочинається з вивчення, розуміння, аналізу й осмислення комп'ютерної системи протягом деякого часу, внаслідок чого, сукупність набутих знань можна з упевненістю іменувати досвідом. Професійно засвоєний інструментарій понять і термінів також свідчить про присутність гносеологічного під час освоєння комп'ютерної системи. Саме він слугує "пропедевтичним курсом" до вивчення комп'ютерних систем і мереж. Адже вправне володіння понятійно-категоріальним апаратом певної науки свідчить про наявність у гносеологічного суб'єкта певного рівня знань.

Не менш важливу роль у процесі пізнання відіграють психологічні особливості самої людини, адже, щоб бути релевантним суб'єктом будь-якої реальності, необхідно передусім бути гносеологічним суб'єктом, основним завданням якого є пізнання тієї реальності, в рамках якої він учиняє певні дії. При скоєнні кібернетичних злочинів таким середовищем виступає віртуальна реальність. Статус гносеологічного підкреслює особливі пізнавальні інтенції суб'єкта, що скеровують його свідомі дії на дослідження певних явищ, процесів чи механізмів. У даному випадку

пізнавальні процеси скеровуються на вивчення особливостей комп'ютерної системи, до якої планує проникнути зловмисник. А саме: а) з'ясовується тип операційної системи та її версія; б) визначаються інстальовані сервіси та додатки; в) розпочинається пошук вразливостей у вищезгаданому програмному забезпеченні. Іншими словами, пізнання є своєрідним "запитом" до дійсності, що вимагає від людини, як суб'єктивної реальності волі максимальної концентрації та спрямованості інтелектуальних зусиль. Перехід "гносеологічного запиту" у соціальну площину з необхідністю видозмінює його, перетворюючи в дію, даючи цим можливість дії безпосередньо впливати на об'єктивну дійсність. Проте, відсутність зумовленості унеможливлює існування дії, адже остання тісно вкорінена в буття суб'єкта. Неможливо уявити яку-небудь дію, яка не походила б від людини та не була результатом складних пізнавальних процесів. У віртуальній реальності "гносеологічний запит" набуває дещо іншої форми і суттєво відрізняється від запиту, що має місце в соціальній дійсності. У процесі вчинення кібернетичного злочину вищезгаданий "гносеологічний запит" розпадається на "пакети даних", які формуються та транслюються у строгій логічній послідовності. Основою цієї віртуальної комунікації виступає протокол, як сукупність обумовлених правил, згідно з якими відбувається передача інформації (запиту). Так запит шляхом комп'ютерної обробки та передачі досягає комп'ютерної системи, яка виступає адресатом запиту і яку планує атакувати кіберзлочинець.

Важливою ознакою пізнавальних процесів є те, що вони мають багатоаспектний характер, тобто є інтенціональними як на усвідомлення смислу здійснюваної активності, так і на безпосереднє виявлення самого механізму дозволених і заборонених форм поведінки. Саме вибір пропонує людині можливі варіанти та форми діяльності, які можуть виявлятися як у правомірній, так і в протиправній поведінці. У гносеологічному сенсі специфіка правомірності та протиправності зіставляється із категоріями істинності та хибності у процесі пізнання. Правомірність розуміється, як слідування людини певним істинніcним правилам, що приводять її до гармонійного спів-буття із соціальною системою. Протиправність же демонструє хибні уявлення суб'єкта про об'єктивну дійсність, а також про способи та засоби її пізнання. Хибність свідчить про спотворення, спрощення, перекручення уявлень людини про емпіричну реальність та її соціальні процеси, вказуючи на найкоротший шлях для задоволення її потреб та інтересів. Обираючи такий шлях, людина опиняється в стані екзистенціальної дезорієнтації, який сприяє формуванню протиправної поведінки в суб'єкта пізнання, автоматично перетворюючи його у злочинця. Дезорієнтований суб'єкт пізнання, опиняючись у такому стані, абсолютно деформує свої уявлення про правові, релігійні, морально-етичні цінності та ідеали, керуючись особистим, суб'єктивно-обмеженим почуттям правильності, міри, межі та відповідальності.

Поняття межі настільки визначене, наскільки ж відносним, зазначав німецький філософ Г. Лейбніц. Питання межі завжди спірне, багатозначне, а найголовніше, суб'єктивне, адже в кожного нас присутнє власне розуміння межі. У віртуальній реальності поняття й ознаки межі не піддаються чіткій та однозначній регламентації. Можемо припустити, що її межі визначатимуться можливостями комп'ютерних систем і мереж, а також гносеологічними здібностями самого суб'єкта. Проте суспільство у процесі пізнавальної активності виробило своєрідні орієнтири правильної поведінки, тобто правові норми, не дотримуючись яких, людина автоматично набуває статусу аутсайдера, який вийшов за встановлені межі гри. Нормативність пізнання набуває свого сконцентрованого правового виразу саме в правовій нормі. Правова норма є найбільш інтенсивним та цілісним проявом гносеологічної природи права, предметом найбільшої пізнавальної напруженості суб'єктів правовідносин. У правовій реальності саме норма права встановлює своєрідну пізнавальну межу, переступивши яку, особа вважається правопорушником, або ж злочинцем.

На підставі вищесказаного можемо з упевненістю стверджувати, що злочин і пізнання тісно пов'язані між собою, адже злочин завжди є пізнанням, пізнанням себе й особливостей середовища, у якому він скоюється. Залежно від специфіки злочинного діяння використовуються різноманітні пізнавальні схеми, які дають змогу злочинцю ліпше освоїти дійсність і виробити власну тактику та стратегію своїх дій. У своїх діях кіберзлочинець стає своєрідним "експериментатором", який випробовує на міцність і стійкість не лише правову, а й віртуальну реальності, намагаючись виявити їх слабкі сторони та прогалини. Сам процес готування до скоєння злочину є комплексом гносеологічно навантажених процедур. Злочинець детально обдумує й обирає засоби та способи, які він планує використовувати у процесі злочинної діяльності; аналізує та моделює різні ситуації, що можуть виникати під час вчинення суспільно небезпечного діяння; скур-

пульозно вивчає комп'ютерну систему та її логіку функціонування, обирає час.

Не менш важливими у процесі гносеологічного аналізу кібернетичних злочинів постають категорії причини та цілі, які заслуговують пильної уваги та детального аналізу. Адже у віртуальному середовищі їх сутність суттєво видозмінюється. Якщо у правовій реальності кожній дії передує певна причина, і ми чітко розрізняємо причину – наслідок, дію – мотив, мету, то у віртуальній реальності категорії причини та цілі можуть з легкістю замінювати одна одну. Причина у віртуальному середовищі може знаходитися безпосередньо в самій меті. Такий стан справ стає можливим завдяки специфіці нелінійних процесів, що мають місце у віртуальній реальності, та дають змогу причині та меті з позиції часу перебувати в одному часовому просторі та в одній часовій точці. У юриспруденції ціль в якості причини не може розглядатися, оскільки юриспруденція розрахована на натуральне вираження певної діяльності.

Як відомо, мета не може вважатись досягненою без наявності засобу. Оскільки останній вважається ключовим елементом при формуванні та досягнення мети. Відсутність правильно підібраного засобу заздалегідь прогнозує крах пізнавального процесу, який так і не в змозі досягти чітко визначеної мети. Тому кіберзлочинець перед початком проникнення до комп'ютерної системи ретельно підбирає засоби та інструменти, які він планує використовувати в процесі своєї діяльності. У рамках скоєння кібернетичного злочину такими засобами та інструментами вважаються комп'ютерні програми, що являють собою набір послідовних інструкцій у вигляді слів, цифр, кодів, схем, символів, виражених у формі, придатній для зчитування та виконання комп'ютерною системою, які приводять його у дію для досягнення певної мети. Такі програми зазвичай можуть бути вже скомпільованими і вимагати запуску у чітко визначеній послідовності, вказавши перед цим координати віддаленої системи, котра планує бути скомпрометованою. Проте бувають випадки, коли злоякісна програма знаходиться у вигляді сирцевого або ж об'єктного коду та потребує попереднього доопрацювання. У такому разі від кіберзлочинця вимагаються напружені пізнавальні зусилля, адже ця ситуація потребує глибоких знань у галузі програмування.

Усе вищесказане підводить нас до з'ясування мети, яку ставить перед собою кіберзлочинець. Адже, саме мета, як глобальна недосяжна ідея дає поштовх кіберзлочинцю постійно та безперервно вдосконалюватися, не даючи йому цим зупинятися на досягненому. Проте дуже часто хибність пізнавального процесу приховується безпосередньо в самій меті або в процесі її досягнення, про що не завжди здогадується кіберзлочинець.

Отже, кібернетичний злочин стає результатом хибності пізнавального процесу, що виступає найкоротшим шляхом до заданої мети. На перший погляд, кібернетичний злочин постає у вигляді цікавої та захоплюючої гри, яка проявляється у формі спортивного та безкорисного інтересу. Такий інтерес з необхідністю викликає відчуття самовпевненості та самовдоволеності, що й призводить до виникнення у свідомості кіберзлочинця стану ейфоричного ефекту.

Проте, окрім безкорисного інтересу, (що має на меті верифікацію отриманих теоретичних знань на практиці та втамування власної пізнавальної жаги) дуже часто має місце корисливий мотив, що виявляє себе в матеріальній зацікавленості кіберзлочинця у вчиненні кіберзлочину. Адже за складними механізмами авторизації та аутентифікації віддаленої комп'ютерної системи знаходиться важлива та недоступна для загалу інформація, висвітлення та розповсюдження якої може мати негативні наслідки. Наприклад: витік інформації про кредитні картки та паролі доступу клієнтів ставить під загрозу авторитет і надійність тієї чи іншої фінансової установи, що суттєво знижує її престиж на ринку фінансових послуг; поява у відкритому доступі облікових даних користувачів однієї з відомих соціальних мереж негативно впливає на її подальшу популярність і закріплює за нею негативну славу, адже в майбутньому кількість користувачів такої мережі значно знижуватиметься, оскільки користувачі шукатимуть безпечнішого притулку для особистої інформації; оприлюднення медичної інформації про стан здоров'я та захворювання пацієнтів ставить під загрозу розкриття лікарської таємниці та може завдати непоправної шкоди честі та гідності особи, яка ні за яких обставин не може бути приниженою. Безумовно, перелік наведених прикладів не є вичерпним, тож може бути суттєво розширеним. Станом на сьогодні інформаційні технології впроваджуються практично в усі сфери людської діяльності, трансформуючи емпірично зафіксовані матеріали в електронні документи, що й робить останні особливо доступними, та неймовірно вразливими.

Переводячи дії кіберзлочинця у площину фундаментальної онтології М. Хайдеггера, можна стверджувати, що завдання кіберзлочинця по-

лягає у "виведенні певного сущого із прихованості", тобто не дати йому можливості маніфестувати свою сутність як щось приховане, потаємне [2, с. 21]. На перший погляд, дана теза немає абсолютно нічого спільного з особливостями кібернетичних злочинів, адже глобальні онтологічні питання навряд чи зацікавлені у розкритті чогось синтетичного та віртуально зорієнтованого, тож на особливий приріст знань годі й розраховувати. Проте своєрідне абстрагування від соціально-емпіричного пласту, яке частково охоплює феномен кібернетичних злочинів, дає змогу глибше осягнути події та процеси, що відбуваються у віртуальному просторі та безпосередньо пов'язані з гносеологічними інтенціями кіберзлочинця.

Під певним сущим у нашому випадку розумітимемо інформацію, що зберігається й обробляється у віддаленій комп'ютерній системі, та є прихованою і недоступною для загального користування. Своїми діями, а саме маніпуляціями із програмним забезпеченням, яке внаслідок чітко визначених логічних операцій взаємодіє із віддаленою комп'ютерною системою, кіберзлочинець отримує доступ до прихованої інформації, знімаючи цим із раніше прихованої інформації статус утаємниченої. Кіберзлочинець немовби "піднімає пізнавальну завісу", за якою приховується інформація. Вчиняючи свої дії в обхід захисних механізмів, кіберзлочинець розширює межі пізнавальних можливостей, збільшуючи так гносеологічні горизонти. То ж унаслідок таких дій усе раніше приховане набуває статусу явного, створюючи так нові можливості для виникнення знань, оскільки доступ до потаємного розкриває злочинцю раніше незвідану інформацію, яка одразу ж перетворюється у нові знання про державні справи, банківські таємниці, приватні взаємовідносини і т.д.

Як бачимо, зміна сущим свого попереднього статусу негативно впливає на його подальше буття та призводить до втрати його попередніх властивостей, адже отримана комп'ютерним злочинцем інформація може бути передана іншим особам, а також оприлюднена у той чи інший спосіб, що може призвести до наслідків, про які йшлося вище. Такі наслідки, безперечно, приводять нас до визначення форми вини, іманентної для кіберзлочинця, який з позицій тієї ж фундаментальної онтології М. Хайдеггера внаслідок причетності до буття "є причиною чогось". А саме: є "власником" своїх дій та цілком усвідомлює їх характер, значення і можливі наслідки. Отже, вина є не зовнішнім фактором, а самим буттям людини [3, с. 75]. Незалежно від реальності, в якій вона перебуває. Чи це соціальна або ж віртуальна, (кібернетична) реальність.

З кримінально-правового погляду, дії кіберзлочинця можна підвести під умисну форму вини. Злочинець розуміє характер своїх дій, а також свідомо бажає настання протиправних результатів. Усе вищесказане не повинно викликати жодних сумнівів, оскільки для скоєння кібернетичного злочину вимагаються особливі знання та вміння, що зумовлюють ретельну підготовку кіберзлочинця, та є результатом складних гносеологічних процесів. То ж питання про форму вини у вигляді необережності заздалегідь виглядає абсурдним і свідчить про хибність пізнавальних процесів дослідника. Проте, як експеримент спробуємо сконструювати ситуацію, яка тісно пов'язана з кібернетичними злочинами та заздалегідь передбачає необережність, як форму вини: користувач, який має безпосередній доступ до комп'ютерної системи, де зберігаються й обробляються важливі дані, з причин власної необережності (причин може бути безліч) чинить певні необдумані дії, внаслідок яких комп'ютерна система починає функціонувати неналежно, порушується логіка роботи операційної системи або ж прикладних програм, що призводить у результаті до повної або ж часткової втрати інформації. Звісно ж, що на кожну тезу знайдеться антитеза, і, беззаперечно, з'являться ті, хто стверджуватимуть, що в нас час, із наявними гносеологічними можливостями будь-яку інформацію з електронних носіїв можна успішно відновити. Але, як свідчить практика системного адміністрування, часто трапляються випадки, коли з тих чи інших причин відновити інформацію стає неможливо, а ні програмними, а ні апаратними засобами. У такому випадку є всі підстави констатувати наявність необережної форми вини у користувача комп'ютерної системи. Адже його необережне та неправильне поводження з комп'ютерною системою призвело до втрати інформації. Проте, чи можна віднести цей випадок до кібернетичного злочину, залишається питанням, оскільки факт втручання відсутній, та й доступ до комп'ютерної системи користувач одержав у правомірний спосіб.

Часто оперуючи термінами, що позначають гносеологічні суб'єкти у кібернетичному просторі, з необхідністю актуалізується питання про їх детальний аналіз і класифікацію, умовно розподіливши їх за гносеологічним та еврестичним потенціалами. Кожен з них по-різному інтерпретує події та процеси, що мають місце у віртуальному середовищі. Тож спробуємо поділити суб'єкти кібернетичного простору на дві групи:

*Користувачі* (до цієї групи належать ті, хто користуються послугами комп'ютерних систем і мереж у науково-практичних, навчальних та інших приватних цілях);

*Системні адміністратори* (ця група охоплює те коло суб'єктів, на яких законом покладено обов'язки обслуговувати та налаштовувати комп'ютерні системи, а також у разі виникнення певних проблем, негайно усувати їх);

Відповідно до запропонованого критерію, з легкістю можна простежити гносеологічні інтенції вказаних суб'єктів. Пізнавальні процеси користувача в більшості випадків спрямовані на пошук і отримання інформації, пов'язаної з явищами, подіями та процесами, які мають місце в суспільстві, державі та навколишньому середовищі. Окрім того, віртуальна реальність дає можливість гносеологічному суб'єкту вільно обмінюватися електронними документами, здавати звіти, працювати з віддаленими базами даних, здійснювати банківські транзакції, тобто використовувати мережеві ресурси у прагматичних цілях. Але ж чи вичерпується на прагматичних цілях потенціал віртуального середовища? Відповідь очевидна, адже зі зміною гносеологічного запиту видозмінюється й віртуальна реальність, перетворюючись із прагматично зорієнтованого середовища у поліфункціональний мультимедійний сервіс, що дає змогу користувачеві зануритись у події улюбленого фільму, ще раз пережити інтригуючі моменти спортивного матчу чи прослухати музику улюбленого виконавця.

Як бачимо, пізнавальна інтесивність користувача комп'ютерної мережі зашишається доволі-таки обмеженою, оскільки дуже часто зосереджується саме на задоволенні особистих потреб та інтересів і може бути безпосередньо пов'язаною із виконанням гносеологічним суб'єктом своїх посадових обов'язків. У зв'язку з цим можемо прийти до висновку, що гносеологічні процеси, які мають місце у свідомості користувача, за своєю природою вузькоспрямовані та предметно обмежені. Адже внутрішні механізми функціонування комп'ютерної мережі не є об'єктом їх зацікавленості, що й створює для них своєрідне обмеження у вигляді "пізнавальної завіси".

Проте існує категорія суб'єктів, для яких пізнання особливостей інфраструктури комп'ютерних систем і мереж є професійним обов'язком, справно дотримуючись якого комп'ютерні системи завжди працюватимуть стабільно, забезпечуючи цим цілодобовий та необмежений доступ для користувачів віддаленої системи. Функція адміністрування, яка є основною в гносеологічній діяльності системного адміністратора, багатоаспектна та не обмежується одним чи двома напрямами діяльності, а охоплює цілий комплекс пізнавально навантажених процедур. А саме: встановлення та конфігурування апаратного та програмного забезпечення; планування та здійснення робіт із розширення мережевої структури на підприємствах, установах та організаціях; створення і збереження резервних копій даних, які обробляються в комп'ютерних системах; завчасне встановлення необхідних оновлень (патчів, заплаток) для операційної системи та прикладного програмного забезпечення; а також відповідальність за інформаційну безпеку комп'ютерної мережі. Звісно, що всі вищезазначені функції адміністрування особливо важливі, адже нехтування хоча б однією із них може призвести до непоправних результатів, що у негативний спосіб відобразяться на функціонуванні комп'ютерної мережі. То ж, згідно з таким станом справ, бачимо, що для успішної реалізації своїх обов'язків системний адміністратор вимушений на професійному рівні володіти усіма напрямами, які входять до функції системного адміністрування. Адже в рамках герменевтичного дискурсу пізнання цілого розпочинається з осягнення його частин. Тобто для успішної гносеологічної діяльності (для пізнання всієї комп'ютерної системи) необхідним постає розуміння її окремих конструктивних елементів, осягнувши які, в системного адміністратора вибудовується цілісна структура комп'ютерної мережі. Очевидно, що в нашому випадку на більш детальну увагу заслуговуватиме останній обов'язок системного адміністратора, оскільки від нього безпосередньо залежить успішність скоєння кібернетичного злочину.

Будь-яка діяльність із захисту комп'ютерних систем і мереж завжди базується на так званій "політиці безпеки", яка розробляється та впроваджується в дію системним адміністратором. Саме від правильно вибраної політики залежить захищеність усієї мережевої інфраструктури, оскільки такі дії вимагають комплексного аналізу та дозволяють виявити наявні вразливості, а також передбачити можливі. Така діяльність вимагає від системного адміністратора напружених пізнавально зорієнтованих зусиль і глибоко аналітичного мислення. Одним із його завдань є моделювання можливих критичних ситуацій, що можуть виникнути із будь-яким апаратним чи програмним механізмом інформаційної системи. Іншими словами, таке моделювання іменується "тестом на проникнення". При реалізації такого тесту відбувається своєрідна підміна гносеоло-

гічними суб'єктами своїх екзистенціальних ролей. Системний адміністратор практично нічим не відрізняється від комп'ютерного злочинця, оскільки ж використовує ідентичні засоби та способи. Ось тільки, на відміну від кіберзлочинця, йому зазделегідь відома мережева топологія, а також інші особливості функціонування комп'ютерної системи. Відмітність становить лише мотиваційна складова, адже своїми діями системний адміністратор має намір виявити прогалини у захисних механізмах комп'ютерної мережі та, в разі їх виявлення, терміново виправити. Корисність такого тесту очевидна, оскільки моделювання нестандартних ситуацій лише зміцнює інформаційну систему, дає змогу адміністратору побувати «по ту сторону барикад». Проте результати такої процедури не до кінця об'єктивні, та можуть піддаватися нищівній критиці. Оскільки системному адміністратору, як нікому іншому, відомі всі події та процеси, що мають місце у його мережі, то ж питання об'єктивної оцінки ставиться під неабиякий сумнів. Для розвіяння будь-яких сумнівів у такій ситуації до аналізу комп'ютерної системи залучається експерт, який виступає в ролі оцінюючого критика, що зобов'язується детально проаналізувати інформаційну систему, та в результаті своєї діяльності надати адміністратору чи керівництву компанії детальний звіт про виконану роботу та виявлені у процесі вивчення і дослідження вразливості.

Тож можемо з упевненістю стверджувати, що весь складний комплекс гносеологічно навантажених дій спрямований на повноцінну реалізацію лише однієї категорії – інформаційної безпеки. Саме безпека сприяє формуванню та виникненню своєрідної пізнавальної межі у віртуальному середовищі, переступивши яку, суб'єкт пізнання автоматично набуває статусу комп'ютерного злочинця, що й стає з погляду позитивного права підставою для притягнення особи до відповідальності. Але, що ж насправді являє собою пізнавальна межа? Що слугує засобом її утворення? Та наскільки реально можна осягнути її абстрактну сутність? Для з'ясування вищезгаданих питань спробуємо звернутися до особливостей функціонування захисних механізмів, а саме: спробуємо зрозуміти, як вони впливають на процес виникнення пізнавальної межі.

Захисні програмно-апаратні комплекси, внаслідок упровадження в інформаційну систему створюють так званий захисний периметр, або ж "захисну оболонку", яка обгороджує всю комп'ютерну мережу, не залишаючи "вільного простору" для несанкціонованого віддаленого втручання. Тобто, створюючи так звану пізнавальну межу, яка не дає змоги користувачеві дізнатися більше, а ніж йому дозволено правилами інформаційної безпеки. Також можуть застосовуватися правила фільтрації запитів, що надходять до комп'ютерної системи, і в разі виявлення підозрілих пакетів даних, такі запити відкидаються та не досягають поставленої мети. Виявлення деструктивних запитів відбувається через наявність певних сигнатур, згідно з якими всі надіслані запити звіряються на предмет відповідності встановлених правил. Чутливість пізнавальної межі теж може піддаватися корегуванню, адже залежно від установленого режиму чутливості залежить реакція захисних механізмів на різноманітні ситуації, що можуть мати місце у мережевій інфраструктурі. Іншими словами, пізнавальна межа залучає до дії захисні механізми в разі потрапляння деструктивних запитів у простір їхньої діяльності, що може свідчити про наявність певної небезпеки. Деструктивний запит – це сформований у чітко визначений спосіб пакет даних, внутрішні властивості та характеристики якого мають намір справити негативний вплив на захисні механізми комп'ютерної мережі. У даному випадку йдеться про пошук слабких місць у інстальованих системах захисту, що дають змогу кіберзлочинцю безперешкодно проникати до файлової системи, а також змінювати параметри захисних механізмів. Отже, отримавши можливість змінювати параметри захисних механізмів, комп'ютерному злочинцю стає можливо змінювати й вищезгадану пізнавальну межу, що пом'якшує дію захисних систем, роблячи їх більш лояльними до деструктивних запитів.

Підсумовуючи вищесказане з приводу критерію класифікації суб'єктів пізнання, доречним буде згадати про його умовність і відносність, адже цілком імовірно, що в рамках іншого пізнавального підходу такий критерій може бути суттєво зміненим, доповненим або ж запереченим. Так що в жодному разі наведений критерій класифікації не претендує на статус істинного, а лише являє собою один із можливих критеріїв класифікації суб'єктів пізнання. Рішення про відсутність категорії кіберзлочинця серед класифікації гносеологічних суб'єктів зазделегідь продумане й обгрунтоване, оскільки будь-хто із користувачів чи системних адміністраторів за певних умов може бути причетним до скоєння кібернетичного злочину, то ж виділяти кіберзлочинця в окрему категорію пізнавальних суб'єктів просто немає сенсу.

**Висновки.** Пізнавальні процеси пронизують увесь соціально-буттєвий устрій людини, торкаючись не лише соціально-правового виміру. Віртуальна реальність, як новітнє середовище спів-буття-з-Іншим створила нові форми між-суб'єктної комунікації, а отже, актуалізувала нові форми пізнавальних процесів. Кібернетичний злочин, як один зі способів пізнання віртуального середовища постає результатом хибності пізнавального процесу, що виступає найкоротшим шляхом до поставленої мети.

**Список літератури**

1. Свасьян К.А. Феноменологическое познание. Пропедевтика и критика : монография / К.А. Свасьян. – М.: Академический Проект; Альма Матер, 2010. – 206 с.

2. Хайдеггер М. Разговор на проселочной дороге : сборник / М. Хайдеггер ; пер. с нем. и ред. А.Л. Доброхотова. - М.: Высш. шк., 1991. – 192 с.

3. Желтова В.П. Философия и буржуазное правосознание : монография / В.П. Желтова. – М.: Наука, 1977. – 103 с.

*Стаття надійшла до редколегії 22 вересня 2015 року.*
*Рекомендована до опублікування у "Віснику" членом редколегії Л.І. Заморською.*

***V.B. Voychyshyn***

**Actualization of onto-gnoseological model of cybercrime**

**Summary**

The article unfolds specificity and peculiarities of the cognitive processes which take place in the cyberspace. They are the result of cognitive activities of the subject and directed to commit cybercrimes. Classification of the gnoseological subjects gives the possibility to understand who commits a cybercrime, under which circumstances and for what reason.

*Keywords:* cognition, cognitive process, gnoseological subject, cybercrime, cyberspace, destructive request, cause, target, guilt.

***В.Б. Войчишин***

**Актуализация онто-гносеологической модели кибернетического преступления**

**Аннотация**

Раскрывается специфика и особенности познавательных процессов, которые имеют место в кибернетическом пространстве, и являются результатом познавательной деятельности субъекта, а также направлены на совершение кибернетических преступлений. Классификация гносеологических субъектов дает возможность более детально понять кто, при каких обстоятельствах и для чего совершает кибернетическое преступление.

*Ключевые слова:* познание, познавательный процесс, гносеологический субъект, кибернетическое преступление, деструктивный запрос, причина, цель, вина.

.