Щит. – М, 1999. – С. 132–133; Расследование преступлений повышенной общественной опасности: Пособие для следователя / Э. Бабаева, А. Гайдук, А. Дворкин и др. / Под ред. Н. Селиванова и А. Дворкина. – М.: Лига-Разум, 1998. – С. 367–368;

7. Щербаковський М.Г. Особливості призначення та проведення комп'ютерно-технічної експертизи // Вісник Національного університету внутрішніх справ. – Х., 2002. – Спецвипуск. – С. 180–181.

8. Абдумаджидов Г.А. Использование научно-технических средств и помощи специалистов (процессуальный аспект) // Труды Ташкентской высш. шк. МВД СССР. – Ташкент: НИиРИО ТВШ МВД СССР, 1976. – С. 9–10; Гончаренко В.И. Научно-технические средства в следственной практике. – К.: Вища школа, 1984. – С. 26–30; Грамович Г.И. Тактика использования специальных знаний в раскрытии и расследовании преступлений: Учеб. пособие. – Минск: МВШ МВД СССР, 1987. – С. 16–21; Кисляков В., Корниенко Н. Предварительные исследования в работе следователя // Соц. закон. – 1972. – № 4. – С. 64–65; Клименко Н.И. Криминалистика как наука. – К.: Правник, 1997. – С. 48; Клименко Н.И. Предварительное исследование рукописных текстов органами расследования и судом для ограничения круга возможных исполнителей // Криминалистика и судеб. экспертиза: Республ. межвед. сб. науч. и науч.-метод. работ. – К.: РИО МВД УССР, 1969. – Вып. 6. – С. 103; Колмаков В.П. Совершенствовать тактику проведения идентификационных следственных действий // Рад. право. – 1968. – № 10. – С. 37; Лисиченко В.К., Циркаль В.В. Использование специальных знаний в следственной и судебной практике: Учеб. пособие. – К.: Изд-во при Киев. ун-те, 1987. – С. 51–55; Порошин Г.Н. О пределах применения криминалистических знаний следователем в процессе предварительного расследования // Использование специальных знаний на первоначальном этапе расследования: Сб. науч. тр. – Волгоград.: ВСШ МВД СССР, 1983. – С. 30; Прищепа В.М., Свалов В.М. Механоскопические диагностические исследования на первоначальном этапе расследования преступлений // Использование специальных знаний на первоначальном этапе расследования: Сб. науч. тр. – Волгоград: ВСШ МВД СССР, 1983. – С. 72; Прищепа В.М., Сегай М.Я. Процессуальные и криминалистические основания идентификационных действий следователя // Криминалистика и судеб. экспертиза: Республ. межвед. сб. науч. и науч.-методич. работ. – К.: РИО МВД УССР, 1969. – Вып. 6. – С. 92–97; Соколовский З.М. О применении следователем криминалистических знаний при исследовании вещественных доказательств // Сов. гос. и право. – 1957. – С. 72–73; Федоров Ю.Д. Специальные познания и формы их использования при расследовании преступлений // Труды Ташкентской высш. шк. МВД СССР. – Ташкент: НИиРИО ТВШ МВД СССР, 1976. – Вып. 9. – С. 21–22.

ГАВЛОВСЬКИЙ В.Д., *кандидат юридичних наук*

ДО ПИТАННЯ ВИКЛАДЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ "ОСНОВИ ТЕОРІЇ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ"

Становлення України як суверенної держави співпало з формуванням у ній інформаційного суспільства: масового впровадження новітніх інформаційних технологій, у тому числі технологій телекомунікації в різні сфери суспільної діяльності. Як і будь-яке соціальне явище інформаційне суспільство має як позитивні так і негативні прояви, зокрема у контексті безпеки життєдіяльності людини, соціальних спільнот, суспільства, держави, міжнародного співтовариства. Формування глобальної інформаційної цивілізації вимагає розробки принципово нових підходів щодо таких суспільних відносин, як інформаційна безпека людини, соціальних угрупувань (корпорацій), держави, суспільства, міжнародного співтовариства. Все це знаходить відображення у праві – множині норм правил поведінки суб'єктів суспільних відноси.

Про рівень публічного усвідомлення інформаційної безпеки, як соціального явища свідчить те, що на законодавчому рівні вона (у відповідності з Концепцією (основами державної політики) національно безпеки України) складає відносно автономну інституцію національної безпеки та є визначною щодо інших провідних складових сфер національної безпеки України: політичної, економічної, соціальної, воєнної, екологічної, науково-технічної.

Категорія “інформаційна безпека” відноситься до багатоаспектних соціологічних та технологічних категорій. Переважно, серед інших аспектів, категорія “інформаційна безпека” може розглядатися за змістом у таких аспектах:

У статичному – як стан захищеності інформаційного середовища суспільства, що забезпечує його формування, використання і розвиток в інтересах людини, організацій, держави, світового співтовариства на певний момент часу (тобто у конкретно визначеному просторі, колу осіб і часі).

У динамічному – як вид суспільних відносин, які виникають у ході забезпечення інформаційної діяльності, що знаходить вираз у відповідних нормативно-правових актах (нормах поведінки, законодавстві, підзаконних нормативних актах).

У науковому – як наукова інституція, предметом дослідження якої є накопичення, аналіз та узагальнення (синтез) знань щодо з’ясування природи, сутності, змісту теоретичних засад та напрацювання рекомендацій практиці щодо забезпечення інформаційної безпеки конкретних суб’єктів суспільних відносин.

Як навчальна дисципліна – покликана передати перевірені практикою теоретичні основи науки і сформувати засади мистецтва організації інформаційної безпеки майбутніми фахівцями у конкретній сфері суспільної діяльності, пов’язаної з інформацією.

Сучасний рівень світового науково-технічного прогресу (НТП) визначається формуванням світової інформаційної цивілізації – стрімким розвитком електронних засобів збору, опрацювання, зберігання та передачі інформації в соціальних системах. Серед електронних засобів інформації сьогодні домінуючу роль відіграють комп’ютерні (цифрові) технології, у тому числі технології телекомунікації.

Поступ НТП у сфері інформаційних технологій знайшов вираз у такому соціальному явищі, яке в сучасній науці отримало назву – електронізація. Черговим етапом електронізації стала її складова – інформатизація. Провідне місце в інформатизації сьогодні займає така її складова як комп'ютеризація: впровадження електронно-обчислювальної техніки (комп'ютерних засобів) в усі сфери соціальних відносин.

Як зазначалося, позитивні здобутки НТП супроводжують і негативні явища: зростання можливості загроз безпеці окремої людини, соціальних спільнот, держави, міжнародного співтовариства від антисоціальних проявів у сфері суспільних інформаційних відносин, засобом вчинення яких є сучасні інформаційні технології. На міжнародному рівні визначається, що загрози інформаційній безпеці окремій людині можуть мати глобальний характер, бути катастрофічними для людства чи окремих регіонів планети. Як приклад, один з багатьох, можна назвати, хоча б розповсюдження шкідливих комп’ютерних програм, які набули умовної назви “комп’ютерні віруси”.

Якщо стихійні (природні) лиха людство ще не навчилося запобігати, то техногенні та соціогенні загрози безпеки знаходяться (щодо упередження, запобігання та боротьби) в межах можливостей людського розуму. Особлива увага сьогодні в теорії і практиці інформаційної безпеки (у обсязі дотримання нормальної життєдіяльності різних суб’єктів суспільних відносин) концентрується на соціальних складових аспектах: передбачення, запобігання, профілактика та боротьба із соціальними та техногенними загрозами. Значна доля в їх структурі належить протидії несанкціонованому (недозволеного, небажаного, неправомірного) доступу до інформаційних ресурсів, зокрема через електронні засоби, автоматизовані (комп’ютерні) інформаційні системи (АІС) чи за їх допомогою.

Мета, мотиви і обставини порушників можуть бути різні:

- навмисне чи необережне пошкодження функціонування інформаційних систем, що призводить до блокування доступу до інформації, або її перекручення;
- крадіжка інформації, що зберігається і циркулює в інформаційній системі, розголошення якої не бажане для законного володільця;

• навмисне чи необережне знищення інформації тощо.

За таких умов постійно існує і зростає потреба та попит на спеціалістів високої кваліфікації, які вміють не тільки створювати та досконало користуватися сучасними електронними засобами у своїй професійній діяльності. Життя вимагає підготовки фахівців, які мають знання і вміють організовувати захист інформації від небажаних для них і суспільства діянь, у тому числі з боку порушників, різними методами та засобами. Це в свою чергу потребує відповідного наукового дослідження, формування теоретичних основ: визначення предмету дослідження, сутності відносин, принципів, методів та відповідного стандартизованого, зрозумілого для всіх понятійного апарату. В свою чергу це забезпечує змістовне, раціональне, логічне формування відповідної навчальної дисципліни.

Програма навчального курсу представляє собою синтез науково-практичних здобутків в різних галузях знань щодо організації захисту інформації – забезпечення інформаційної безпеки на відповідному рівні соціального буття, його структури, підсистем: окремої людини; соціальних спільнот (організацій), держави тощо. При вивчені проблематики інформаційної безпеки слід також враховувати міжнародні аспекти захисту інформації: регіональні, континентальні, глобальні. Щодо останніх - значну роль у них все більше і більше відіграють такі засоби комунікації, як Інтернет.

Програма поєднує комплекс проблематики, з різних, нерозривних в практиці наукових підходів: управлінського; правового; інженерно-технічного, у тому числі технологічного та інших. Всі вони розглядаються як складові теорії організації (тектології) інформаційної безпеки – *міжгалузевої комплексної синтетичної науки (чи навчальної дисципліни), щодо суспільних відносин, які знаходять вираз у оптимізації заходів, дій, методів відповідних суб'єктів (людини, соціальних спільнот, держави), для створення (організовування) необхідних, нормальних, безпечних умов функціонування окремих видів інформаційних систем.*

Мета програми полягає в тому, щоб надати допомогу тим, хто вивчає дану навчальну дисципліну в освоєнні комплексу теоретичних знань та здобуття практичних навичок щодо організації захисту інформації, як складової забезпеченні інформаційної безпеки відповідного рівня інформаційних відносин та соціального управління ними.

Здобуття знань, які прийдеться застосовувати у майбутній професійній діяльності, потрібно не тільки звичайним користувачам інформаційних систем, але і, можливо, організаторам (менеджерам, управлінцям, керівникам) відповідних організаційних структур, зокрема, щодо інформаційного забезпечення їх безпечного, нормального функціонування.

Завдання програми поділяються на провідні і спеціальні.

Провідними завданнями є здобуття знань щодо основ науки і мистецтва організації інформаційної безпеки на відповідному рівні соціальної організації: людини, корпорації (підприємства, установи організації), суспільства, держави, міжнародного співтовариства.

Спеціальні завдання. Зміст проблематики програми умовно поєднує (інтегрує) три нероздільні в практиці напрямки, які визначають спеціальні завдання навчальної дисципліни: організаційно-управлінські, організаційно-технічні та організаційно-правові:

• перші - об’єднують питання щодо завдань організовування та керування забезпечення інформаційної безпеки – захисту інформації у відповідних інформаційних системах (персональних, корпоративних, державних тощо);

• другі – містять комплекс завдань щодо визначення принципів організації забезпечення інформаційної безпеки технічними засобами, в контексті науки інформатики та інших технічних наук;

• треті – містять питання правового регулювання забезпечення організації інформаційної безпеки в рамках комплексного міжгалузевого юридичного інституту – інформаційного права, що формується на основі існуючої доктрини поділу права на публічне і приватне,

матеріальне і процесуальне, а також провідних галузей державного права: конституційного, адміністративного, цивільного, трудового та кримінального.

Викладання і вивчення тематики програми навчальної дисципліни базується на тому, що ті, хто її вивчає, мають базові знання з основ інформатики і обчислювальної техніки, основ права. Положення зазначених дисциплін розглядаються у контексті основ теорії управління соціальними системами, зокрема тектології (теорії організації соціальних систем) тощо.

В свою чергу, знання на навички щодо тем даного навчального курсу дозволить більш усвідомити знання тематики інших навчальних дисциплін, що вивчаються у вищому навчальному закладі, зокрема загально-юридичних (провідних галузей державного права: конституційного, адміністративного, цивільного, трудового та кримінального), спеціальних дисциплін щодо питань теорії психології управління соціальними системами, організації професійної діяльності тощо.

Навчальний курс за програмою передбачає курс лекцій, семінарські, практичні (лабораторні) та самостійні заняття під керівництвом викладачів-спеціалістів. Розподіл часу на вивчення тем програми зазначається в тематичному плані з урахуванням фахової спеціалізації.

Розроблений на основі Програми навчальний план включає завдання рекомендаційного змісту для самостійної роботи тих, хто навчається, щодо тем курсу: з літературними джерелами, відповідними технічними засобами, у тому числі з персональним комп'ютером, Інтернет. Це сприятиме більш глибокому засвоєнню основного матеріалу програми і дозволяє набути стійких теоретичних знань і практичних навичок щодо захисту інформації, інформаційної безпеки.

Якщо навчальний курс за Програмою має відкритий зміст, в ньому забороняється використовувати інформацію з обмеженим доступом (у відповідності із Законами України “Про інформацію”, “Про державну таємницю” та іншими нормативно-правовими актами).

Програмою підготовки фахівців повинна передбачатися можливість ознайомлення під час стажування з практикою щодо питань організації інформаційної безпеки, захисту інформації.

Викладач за погодження з кафедрою має право на творчу ініціативу, зокрема, вносити обґрунтовані зміни у зміст та розподіл часу під час аудиторних занять у межах загального бюджету аудиторного навчального часу, виділеного на вивчення Програми. Це здійснюється в залежності від профілю підготовки спеціаліста, матеріально-технічного забезпечення вузу та інших навчальних дисциплін, окремі теми яких подібні за змістом.

У зв'язку з тим, що в Україні проблематика навчального курсу ще не знайшла достатнього висвітлення у науково-практичній літературі на державній мові (на рівні монографій, посібників, підручників) то у бібліографії подаються переважно російськомовні джерела.

Слід також зазначити, що проблематика програми відноситься до таких соціальних відносин, які бурхливо розвиваються: як в інженерно-технічному, так і в організаційно-правовому аспектах. Це потребує відповідного моніторингу інформації, відслідковування новацій у теорії і практиці організації інформаційної безпеки. У зв’язку із зазначеним викладачем стимулюється і заохочується творчий пошук студентів щодо пошуку новацій з проблематики навчального курсу. Студенти до аудиторних занять готують реферативні виступи з питань тем, зазначених у програмі, у визначеному викладачем порядку.

Викладання навчальної дисципліни здійснюється за методикою ступеневого здобуття знань. На лекціях викладач, через визначення комплексу питань, формулює проблеми щодо теми та її теоретичні засади. Під час самостійної роботи студенти шукають додаткову інформацію щодо визначених у програмі питань і поглиблюють свої знання. На семінарських (практичних) заняттях проводиться обговорення проблем за принципом партнерства.

Використана література

1. Айков Д., и др. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями: Пер.с англ. – М.: “Мир”, 1999.

2. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юрид. лит., 1991.

3. Вакка Дж. Секреты безопасности в Internet. – К.: “Диалектика”, 1997.

4. Виявлення та розслідування злочинів, що вчиняються за допомогою комп`ютерних технологій. Посібник /Романюк Б.В. Камлик М.І., Гавловський В.Д., Хахановський В.Г. Цимбалюк В.С. /За ред. Я.Ю.Кондратьєва. – К.: НАВСУ, 2000. – 64 с.

5. Гавловський В.Д., Цимбалюк В.С. Щодо проблем боротьби із злочинами, що вчиняються з використанням комп’ютерних технологій // Боротьба з контрабандою: проблеми та шляхи їх вирішення. - К.: НДІ "Проблем людини",1998. – С.148-154.

6. Калюжный Р.А. Научно-технический прогресс в деятельности правоохранительных органов. – К.: “Наукова думка”, 1990.

7. Калюжний Р.А., Цимбалюк В.С. Вдосконалення інформатизації ОВС України - передумова покращення їх діяльності в боротьбі зі злочинністю // Правова система України: теорія і практика. 1993. – С.397-399.

8. Кримінальне право. Особлива частина. Підручник. (Александров Ю.В., Антипов В.І. та інші). Відпов. редактор Шакун В.І. – К.: “Правові джерела”, 1999.

9. Уголовный кодекс Украины: Научно-практический комментарий (Ответ. Редакторы Яценко С.С., Шакун В.И.). – К.: “Правові джерела”, 1998.

10. Ярочкин В.И. Безопасность информационных систем. – М.: “Ось-89”, 1996.

11. Ярочкин В.И. Информационная безопасность. Учебное пособие. – М.: Международные отношения, 2000. – 400 с.

В.ХАХАНОВСЬКИЙ, *кандидат юридичних наук, доцент*

НАУКОВО-ПЕДАГОГІЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БОРОТЬБИ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ В ІНФОРМАЦІЙНІЙ ТА КОМУНІКАЦІЙНІЙ СФЕРАХ

Людство неминуче вступає в інформаційну епоху. Фахівці вважають, у світі розпочалося сторіччя інформатизації. Не стоїть осторонь цього процесу й наша держава, де останніми роками питанням інформатизації суспільства приділяється особлива увага.

Загальновідомий вислів “Хто володіє інформацією, той володіє світом” у значній мірі стосується правоохоронних органів, де процеси збирання, обробки, аналізу та зберігання інформації, на основі якої приймаються управлінські рішення, відіграють вирішальну роль.

Сьогодні в Україні спостерігається інтенсивне впровадження сучасних інформаційних технологій в діяльність правоохоронних органів. Створюються міжвідомчі інформаційні системи правоохоронних органів, які успішно використовуються у боротьбі зі злочинністю. На відомчі навчальні заклади покладено відповідальне завдання – підготовка висококваліфікованих фахівців нового тисячоліття, спроможних орієнтуватися в величезних інформаційних потоках, адекватно протистояти злочинним угрупованням, які сьогодні мають сучасне технічне оснащення та спеціальну підготовку.

Боротьба зі злочинністю в інформаційній та комунікаційній сферах набула особливої гостроти та актуальності в усьому світі. Так, за даними Федерального міністерства внутрішніх справ Німеччини, за останні 10 років кількість таких злочинів там зросла у 10 разів. Лише в Баварії за 1999 рік вчинено 4451 злочин цього виду, у 2000 році тільки в м. Мюнхені порушено вже біля 300 кримінальних справ, пов’язаних з такими злочинами.

У зв’язку з різким поширенням цього виду злочинів у всьому світі нині існують чи створюються відповідні підрозділи по боротьбі з ними. Наприклад, у тій же Німеччині функціонують підрозділи з вилучення речових доказів комп’ютерних злочинів. Позитивні зміни у