ЗАХИСТ ІНФОРМАЦІЇ

УДК 638.253.2:612.931

О.В. Рибальський, доктор технічних наук, професор,
В.О. Хорошко, доктор технічних наук, професор ДУІКТ,
М.Є. Шелест, доктор технічних наук, професор ДУІКТ,
І.І. Орєхова

МЕТОДОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ПІДГОТОВКИ СПЕЦІАЛІСТІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті викладено питання науково-методологічного забезпечення підготовки кадрів з інформаційної безпеки з метою удосконалення теорії захисту.

Ключові слова: *інформаційна безпека, науковий підхід, комплексний захист інформації, методологічне забезпечення, підготовка кадрів.*

В статье изложены вопросы научно-методологического обеспечения подготовки кадров по информационной безопасности с целью усовершенствования теории защиты.

Ключевые слова: *информационная безопасность, научный подход, комплексная защита информации, методологическое обеспечение, подготовка кадров.*

In this article the questions of scientific-methodological provision of professional training in the sphere of information security are defined with the aim of security theory improvement.

Keywords: *information safety, scientific approach, complex protection of information, methodological maintenance, professional training.*

У сфері інформаційної безпеки до сьогодні накопичено чималий досвід як у сфері теоретичних досліджень, так і в області практичного вирішення завдань захисту в системах різного рівня і призначення. З метою узагальнення наявного досвіду й подальшого розвитку концепцій, методів і засобів захисту були проведені наукові дослідження в декількох вузах України. На підставі цих досліджень були розроблені державні стандарти для підготовки бакалаврів за напрямом 1701 "Інформаційна безпека", а нині здійснюються роботи з розробки стандартів для магістрів. Крім цього, й надалі удосконалюється теорія захисту інформації, зокрема, проблеми перспектив розвитку, концепції, методів і засобів захисту.

На підставі виконаної роботи сформульовано п'ять принципів значущості:

1) на цей час (і тим більше в перспективі) необхідний виключно науковий підхід до вирішення проблем інформаційної безпеки. Панівний емпіричний підхід свої можливості вичерпав повністю і вже не відповідає об'єктивним потребам сьогодення. Водночас у рамках емпіричного підходу створено об'єктивні передумови, необхідні для формування основ наукового підходу;

2) за сучасних умов, як і в майбутньому, найбільш ефективним буде комплексний захист, причому як за цілями (забезпечення фізичної й логічної цілісності, попередження несанкціонованих модифікацій, отримання й розмноження інформації під захистом), так і за засобами захисту, що використовуються (технічні, програмно-апаратні, організаційні, принтографічні);

3) проблеми захисту інформації в сучасних системах її обробки ефективно не можуть бути вирішені окремо від тих інформаційних процесів, при здійсненні яких необхідний захист. Надійний захист може бути забезпечений лише за умови повної структуризації процедур збору, передачі, нагадування, зберігання, пошуку, переробки та видачі інформації під захистом;

4) для забезпечення ефективного захисту необхідна чітка організація й усебічне забезпечення всіх робіт, що проводяться з метою захисту;

5) основні роботи із захисту інформації мають суто специфічний та індивідуальний характер, тому ефективно можуть бути виконані лише спеціалістами-професіоналами у сфері інформаційної безпеки. Відповідно, для регулярного кадрового забезпечення всіх зацікавлених організацій необхідна стрункa система підготовки, перепідготовки й підвищення кваліфікації відповідних спеціалістів.

Отже, у якості основних обрано такі питання підготовки кадрів:

– передумови вирішення проблеми, що розглядається;

– перелік категорій фахівців, які потребують спеціальної підготовки з проблем інформаційної безпеки, і необхідного рівня підготовки;

– концептуальні підходи до формування навчальних планів з інформаційної безпеки;

– проблеми, пов'язані з методичним забезпеченням підготовки кадрів, та шляхи їх подолання.

Розглянемо більш детально кожне з перелічених питань.

Передумови вирішення проблеми підготовки кадрів. Основним у цих передумовах є наявність достатньо фундаментальних результатів теоретичних досліджень проблем захисту інформації, досвіду практичного рішення захисту й досвіду підготовки кадрів відповідного профілю у вузах України.

Результати теоретичних досліджень у повному вигляді представлено в роботах [1, 2, 3], де сформульовані основні принципи побудови інформаційної безпеки в Україні та вимоги до підготовки спеціалістів. У цих матеріалах сформовано за-гальну структуру теорії захисту й обґрунтовано її основні концептуальні положення. Показано, що вся незліченна кількість потенційних вимог до захисту може бути задоволена за умови, що будуть розроблені три стратегії: оборонна (захист від виявлених загроз), наступальна (захист від усіх потенційно можливих загроз) та стверджувальна (створення захищеного інформаційного середовища). Предметно показані не тільки можливості реалізації зазначених стратегій вже наявними засобами, але й їх реалізація на базі єдиної концепції захисту, що забезпечує уніфікованість підходу до організації і захист інформації на різних об'єктах та в різних умовах їх функціонування. Така концепція називається уніфікованою, і основні її положення розроблені досить детально й викладені в роботах [4, 5].

Цікаво буде відзначити, що розширення рамок оборонної стратегії природним чином призводить до стратегії наступальної, а розвиток умов, що сприяють підвищенню ефективності захисту інформації в рамках наступальної, до створення відповідного інформаційного середовища, тобто переходу до стверджувальної стратегії. Тому найбільш перспективною є стверджувальна стратегія захисту, що передбачає створення захищеного інформаційного середовища, у якому завдання захисту інформації мають органічно включатися до загального переліку завдань її обробки, а необхідні для цього засоби – в архітектуру відповідних інформаційних технологій. Однак, як показали дослідження, створення захищеного

інформаційного середовища можливе лише за беззастережного вирішення низки нетривіальних проблем: уніфікації структури інформаційних потоків і процедур обробки інформації, стандартизації методів обробки інформації, побудови й використання інформаційних технологій тощо.

Зазначені проблеми, незважаючи на їх чималу складність і неординарність, нині знайшли своє рішення, на основі якого розроблено так звану уніфіковану технологію автоматизованої обробки інформації (УТАОІ). Структура, загальний зміст та питання практичного використання УТАОІ викладено в роботі [6]. Завдяки уніфікованості та стандартизованості основних концептуальних рішень УТАОІ виявилась повністю структурованою, що створює надзвичайно сприятливі передумови для побудови ефективних механізмів захисту інформації та регулярного управління ними в процесі функціонування УТАОІ.

Важливими теоретичними передумовами проблеми, що розглядається, є також результати досліджень і розробок засобів захисту інформації (технічних, програмно-апаратних, організаційних, криптографічних) та засобів проектування систем захисту інформації.

Велике значення для створення науково обґрунтованої системи підготовки кадрів з інформаційної безпеки має накопичений досвід розробки і практичного використання різних засобів захисту та вирішення завдань захисту в системах різного рівня (від загальнодержавних до невеликих об'єктних) і різного призначення (від урядових до комерційних). Як відомо, цими питаннями досить професійно займаються багато організацій як державного, так і недержавного характеру. Узагальнені дані з практики рішень проблем інформаційної безпеки містяться в публікаціях [7, 8, 9]. Слід наголосити, що завдання серйозної аналітично-синтетичної обробки даних досвіду інформаційної безпеки ще очікує на своє рішення.

Важливий вклад у скарбницю цих передумов зробила і продовжує робити практика підготовки, підвищення кваліфікації та перепідготовки кадрів із інформаційної безпеки. Як відомо, донині в багатьох вузах України вже склалася система підготовки молодих спеціалістів зі спеціальностей, що належать до інформаційної безпеки. У ході навчального процесу та навчально-методичної роботи сформовано й апробовано навчальні програми з цілої низки дисциплін, а також видано підручники й навчальні посібники. Однак ця робота ще далека від завершення і задовільного стану.

Перелік категорій спеціалістів, які потребують спеціальної підготовки з інформаційної безпеки. Донедавна інформаційною безпекою займалися майже виключно спеціалісти-професіонали у сфері захисту. Це положення практично є чинним і на цей час. Таке ставлення до проблеми захисту однозначно відобразилося й у практиці підготовки кадрів. Спеціальна підготовка охоплює переважно спеціалістів-професіоналів. Щоправда, у деяких вузах України читають курси із захисту інформації студентам інших спеціальностей. Таке ставлення до підготовки було якщо не виправданим, то більш-менш допустимим доти, доки традиційні й автоматизовані технології обробки інформації функціонували майже незалежно одна від одної, а її захист зводився переважно до запобігання несанкціонованому отриманню інформації зловмисниками. Проте нині, коли традиційні й автоматизовані технології обробки інформації все більше інтегруються в єдину, причому засоби обчислювальної техніки (ПЕОМ, ноутбуки, смартфони тощо) набувають масового поширення, коли ефективним може бути тільки комплексний захист, причому як за метою, так і за засобами захисту, у забезпеченні захисту інформації мають активно брати участь не лише фахівці-професіонали, але тією чи іншою мірою всі особи, які займаються обробкою інформації й використовують її. Крім цього, оскільки арсенал методів та засобів захисту неухильно зростає й стає все більш розмаїтим, то й у середовищі професіоналів у сфері інформаційної безпеки

необхідна спеціалізація за класами засобів захисту, а для вирішення загальносистемних питань постає необхідність підготовки системотехніків із захисту інформації.

Із викладеного вище випливає, що в системі підготовки кадрів з інформаційної безпеки спеціальну підготовку мають проходити наступні категорії спеціалістів:

1) керівники підприємств, установ і організацій;
2) спеціалісти, що займаються обробкою інформації;
3) керівники служб безпеки підприємств, установ і організацій;
4) робітники режимно-секретних підрозділів;
5) системотехніки із захисту інформації;
6) спеціалісти з технічного захисту;
7) спеціалісти з програмно-апаратного захисту;
8) спеціалісти з організаційно-правового захисту;
9) спеціалісти з криптографічного захисту;
10) науково-педагогічні кадри у сфері інформаційної безпеки.

Концептуальні підходи до формування навчальних планів підготовки спеціалістів із інформаційної безпеки. На формування зазначених підходів значною мірою впливають такі обставини:

– у навчальних планах мають бути відображені не тільки останні досягнення в сфері захисту інформації, але й перспективи розвитку відповідних концепцій;

– навчальні плани та програми мають відповідати об'єктивним потребам підготовки спеціалістів різних категорій;

– навчальні плани та програми підготовки спеціалістів різних категорій мають будуватися на єдиній науково-методичній базі.

Відповідно до наведених вимог, в основу концептуальних підходів до формування навчальних планів покладено принципи формування базового плану, єдиного для підготовки всіх категорій; відмінності в обсязі та змісті програм для спеціалістів різних категорій мають братися до уваги при плануванні кількості годин, призначених для вивчення різних розділів навчального плану, і формуванні змісту навчальних програм відповідних дисциплін.

Зразкову структуру базового навчального плану наведено на мал. 1. Структура і зміст програм, передбачених в базовому плані дисциплін, можуть бути сформульовані на основі досвіду їх вивчення (або аналогічних їм) у вузах, де ведеться підготовка спеціалістів з інформаційної безпеки. Розподіл навчального часу між дисциплінами може бути гнучким аж до обліку рівня підготовки студентів або слухачів конкретних навчальних груп.

Основне призначення і загальний зміст виділених блоків базового учбового плану полягає в наступному.

1. Вступ в інформаційну безпеку

Інформаційна безпека виконує забезпечувальну функцію відносно інформаційних процесів, тобто процесів інформаційного забезпечення різних сфер діяльності суспільства. Звідси випливає, що вирішення завдання захисту має точно узгоджуватися з вирішенням завдань обробки інформації. Відповідно, спеціалісти, які беруть участь у вирішенні завдань захисту, неодмінно мають знати принципи і методи організації інформаційних процесів. Тому основна дисципліна блоку, що розглядається, має назву "основи теорії інформатики та інформатизації". При цьому, на відміну від ототожнення інформатики з розвитком та використанням обчислювальної техніки, що набуло широкого поширення,

тут інформатика трактується як науковий напрям, цілі якого полягають у вивченні інформаційних проблем суспільства і розробці способів, методів і засобів найбільш раціонального їх вирішення. Іншими словами, інформатика розглядається як науково-методологічний базис інформатики суспільства, тобто організації інформаційного забезпечення діяльності в різних сферах життя. Що стосується принципів і методів використання сучасних засобів ВТ, то знання про них та володіння ними є абсолютно необхідними для спеціалістів із інформаційної безпеки, але отримання цих знань та навичок має передувати вивченню основ теорії інформатики та інформатизації і в рамках самостійних навчальних дисциплін.

Багаторічний аналіз теоретичних і практичних робіт показує, що на цей час постала необхідність реалізації концепції захисту інформації, а для цього є важливим вивчення основ інформаційної безпеки. Знання та її реалізація дозволяє забезпечити необхідний рівень захищеності інформації.

Руйнування важливої інформації, викрадення конфіденційних даних, перерва у роботі внаслідок втручання у функціонування систем різного призначення – усе це виливається у великі матеріальні втрати, завдає шкоди репутації підприємств, установ та організацій. Проблеми, пов'язані із системами керування, загрожують державі, суспільству, а також здоров'ю й життю людей.

Основи інформаційної безпеки підводять студентів до вирішення проблем і завдань інформаційної безпеки, дозволяють їм осягнути багатофункціональність і особливість цієї проблеми.

1.Вступ в інформаційну безпеку			
Основи теорії інформатики та інформатизації	**2.Методологія захисту**		
Основи інформаційної безпеки	Методи та засоби ЗІ	**3. Засоби захисту інформації**	
	Політика інформаційної безпеки	Засоби технічного захисту інформації	**4.Організація захисту інформації**
	Нормативне забезпечення інформаційної безпеки	Програмні засоби ЗІ	Проектування комплексних систем ЗІ
	Правові основи охорони інформації	Криптографічний ЗІ	Управління інформаційною безпекою
	Стратегія управління інформаційною безпекою	Організаційно-технічне забезпечення ЗІ	
		Спеціальні вимірювання	

Рис. 1. Узагальнена структура базового навчального плану з інформаційної безпеки

2. Методологія захисту

Як випливає із самої назви блоку, головна мета його полягає в тому, щоб дати студентам найбільш повне і систематизоване уявлення про суть проблем інформаційної безпеки, а також про способи, методи й засоби раціонального їх вирішення. Крім цього, вони мають бути обізнані у правовому та нормативному забезпеченні інформаційної безпеки. Також розробка політики інформаційної

безпеки – це нетривіальне питання. Від ретельності його опрацювання залежатиме дієвість решти всіх рівнів забезпечення інформаційної безпеки – процедурного і програмно-технічного. Складність розробки політики безпеки визначається проблематичністю використання чужого досвіду, оскільки політика безпеки ґрунтується на виробничих ресурсах і функціональних залежностях всередині об'єкта захисту.

3. Засоби захисту інформації

Призначення цього блоку є очевидним, а його загальний склад представлено на наведеному малюнку. Очевидно, що для вивчення кожного виду засобів доцільно було б передбачити самостійну навчальну дисципліну, причому в програмах цих дисциплін є необхідним вивчення як системних питань відповідних засобів (принципи побудови, призначення і можливості, системна класифікація, ефективність, техніко-економічні показники), так і пристроїв, роботи і правил використання конкретних зразків відповідних засобів.

4. Організація захисту

Основне призначення цього завершального блоку дисциплін полягає в систематизації всіх знань і навичок, отриманих в процесі вивчення дисциплін попередніх блоків, і формуванні на цій основі цілісного уявлення про способи і методи практичної реалізації систем захисту. Як показано на рис.1, у цьому блоці виокремлено дисципліни, в рамках яких передбачається вивчення способів і методів організації комплексного захисту сучасних об'єктів, тобто підприємств, установ і організацій різного рівня та профілю, а також проектування і розробка таких систем та управління самим процесом захисту.

Проблеми методичного забезпечення підготовки кадрів з інформаційної безпеки та шляхи їх подолання. Як нескладно переконатися, наведена вище концепція підготовки кадрів передбачає створення досить складної і широко розгалуженої системи навчального процесу. Немає необхідності доводити, що неодмінною умовою ефективного функціонування цієї системи є адекватне їй методичне забезпечення, яке можуть надати лише великі вузи, з добре налагодженою навчально-методичною базою і спеціальним підбором викладачів. До основних компонентів зазначеного забезпечення слід віднести:

1) програми дисциплін базового навчального плану з конкретизацією кожної програми для кожної категорії спеціалістів;

2) плани семінарів і лабораторних робіт з кожної дисципліни;

3) методичні матеріали для викладачів із проведення занять із кожної дисципліни;

4) методичні вказівки студентам із вивчення відповідних дисциплін;

5) підручники та навчальні посібники з кожної дисципліни.

При цьому наведені вище компоненти мають бути не розрізненими, а створювати єдину систему методичного забезпечення та спиратися на розвинену лабораторно-експериментальну базу. На жаль, таке забезпечення практично відсутнє у багатьох вузах. Достатньо зазначити, що до сьогодні видано дуже мало підручників з інформаційної безпеки. Такий стан не тільки не відповідає сучасній постановці завдання підготовки кадрів з інформаційної безпеки, а й може стати серйозною перешкодою на шляху ефективного вирішення цього завдання. Звідси випливає, що формування науково-методичного забезпечення зазначеної проблеми підготовки кадрів має бути віднесене до проблем, пріоритетних за значимістю і першочергових за строками розробки.

Висновки

Усвідомлюючи таку значимість і нагальність проблеми формування науково-методологічного базису і прагнучи зробити вагомий вклад у її вирішення, деякі вузи України об'єднали свої зусилля, а саме: Національний університет "Львівська політехніка"; Вінницький національний технічний університет; Східноукраїнський національний університет ім. В. Даля; Харківський національний університет радіоелектроніки; Севастопольський національний університет ядерної енергії та промисловості; Військовий інститут Київського національного університету ім. Т.Шевченка; Військовий інститут телекомунікацій та інформатизації НТУУ "КПІ" та Державний університет інформаційно-комунікаційних технологій. Одним із перших результатів за цим напрямом став випуск підручника "Методологічні засади викладання інформаційної безпеки у вищих навчальних закладах" (СНУ ім. В. Даля та ДУІКТ у 2010 році). Крім того, розроблено та впроваджено Галузеві стандарти вищої освіти для бакалаврів у галузі знань 1701 "Інформаційна безпека", а також написано та надруковано підручники за низкою базових дисциплін.

У планах роботи вузів найближчим часом передбачено розробку та видання підручників і навчальних посібників з дисциплін навчального плану і достатньо повної системи навчальних посібників та інших компонентів навчально-методичного забезпечення.

Надаючи великого значення створенню гарної експериментальної бази, у практичній площині розглядається питання про створення Міжгалузевого навчально-наукового дослідного центру з комплексного захисту інформації на базі комплексного науково-дослідного відділення захисту інформації "Бар'єр" публічного акціонерного товариства "Науково-дослідний інститут електромеханічних приладів". У роботі цього центру мають брати активну участь фахівці ПАТ "НДІЕМП", ТОВ "ЕПОС", НВП "РІАС", ДУІКТ та ВІ КНУ ім. Т. Шевченка. З досвіду практичної роботи найбільш оптимальною структурою для здійснення такої роботи є поєднання спеціальних вузів та підприємств, які активно співпрацюють в галузі інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Концепція технічного захисту в Україні : Постанова Кабінету Міністрів України № 1126 від 08.10.1997.

2. Про доктрину інформаційної безпеки України : Указ Президента України від 08.07.2009 № 514/2009.

3. Положення про Адміністрацію Державної Служби спеціального зв'язку та захисту інформації України : Затверджено Указом Президента України від 30.06.2011 № 717/2011.

4. *Герасименко В.А.* Защита информации в автоматизированных системах обработки данных : у 2-х тт. / В.А. Герасименко. – М. : Энергоатомиздат, 1994.

5. *Лєнков С.В.* Концептуальні і методологічні підходи до підготовки спеціалістів з інформаційної безпеки / С.В. Лєнков, І.І. Орєхова, В.О. Хорошко.

6. *Герасименко В.А.* Основы информационной грамотности / В.А. Герасименко. – М. : Энергоатомиздат, 1995. – 438 с.

7. *Ленков С.В.* Методы и средства защиты информации : в 2-х тт. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К. : Арий, 2008.

8. *Голубенко О.Л.* Особливості підготовки фахівців з інформаційної безпеки в Україні / О.Л. Голубенко, О.С. Петров, В.О. Хорошко // Інформаційна безпека. – 2009. – № 2. – С. 5–17.

9. *Махоніна О.* Підготовка фахівців у сфері інформаційної безпеки / О. Махоніна // Бизнес и безопасность. – 2011 – № 3. – С. 88–100.

Отримано 13.12.2011