/ Н.Л. Иванова // Вопросы психологии. – 2008.– № 1. – С. 89-100.
3. Иванова, С.П. Учитель XXI века: ноопсихологический подход к анализу профессионально-личностной готовности к педагогической деятельности [Текст] / С.П. Иванова. – Псков: ПГПИ им. С.М. Кирова, 2002. – 228 с.
4. Макарова, И.К. Управление человеческими ресурсами: пять уроков эффективного HR-менеджмента [Текст] / И.К. Макарова. – М.: Дело, 2007. – 232 с.
5. Ньюстром, Д.В. Организационное поведение [Текст] / Д.В. Ньюстром, К. Дейвис; пер. с англ. под ред. Ю.Н. Каптулевского. – СПб: Питер, 2000. – 346 с.
6. Персикова, Т.Н. Межкультурная коммуникация и корпоративная культура: [учебное пособие] [Текст] / Т.Н. Персикова – М.: Логос, 2002. – 224 с.
7. Скрипкина, Т.П. Психология доверия: [учебное пособие для студ. высш. пед. учеб. заведений] [Текст] / Т.П.Скрипкина. – М.: Издательский центр «Академия», 2000. – 264 с.

КАСЯРУМ Я.О.,
інженер-програміст Черкаського інституту банківської справи Університету банківської справи Національного банку України

УДК 378.14

ДОТРИМАННЯ ВИМОГ СИСТЕМИ БЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ ЯК СКЛАДОВА ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ МАЙБУТНЬОГО ЕКОНОМІСТА

У статті розглянуто існуючі вимоги сучасної системи безпеки корпоративної інформації, в умовах якої майбутній економіст повинен працювати.
Ключові слова: майбутній економіст, вимоги системи безпеки, корпоративна інформація.
В статье рассмотрены существующие требования современной системы безопасности корпоративной информации, в условиях которой будущий экономист должен работать.
Ключевые слова: будущий экономист, требования системы безопасности, корпоративная информация.
The existent requirements of the modern system of safety of corporate information which a future economist must work in the conditions of are considered in the article.
Key words: future economist, requirements of the system of safety, corporate information.

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Процеси глобалізації у світовій економіці, що призвели до доступності фінансових послуг усі 24 години на добу, незважаючи на існуючі кордони, ґрунтуються на сучасних телекомунікаційних та інформаційних технологіях. Їх упровадження стало практикою життєдіяльності всіх організацій завдяки обміну електронними даними та електронному документообігу. «Обмін електронними даними – це умова діяльності банку, фірми, це обмін діловими, комерційними, фінансовими документами» [1, с. 343]. Оскільки певну частину інформації (залежно від типу організації) складає інформація з обмеженим доступом, то виникає потреба в її захисті. Це завдання покладається на співробітників служби безпеки та на персонал організації.

Виділення невирішених раніше частин загальної проблеми, яким присвячується означена стаття. Випускники економічних факультетів після завершення процесу професійної підготовки працюють на підприємствах державної і приватної форми власності. «Приховане безробіття» часто призводить до необхідності працювати не за здобутою спеціальністю, а там, де є робота. Ми відносимо «приховане безробіття» і «роботу не за спеціальністю» до соціальних чинників, які впливають на працевлаштування майбутнього економіста. Водночас його конкурентоспроможність визначається й навчальним планом професійної підготовки, яка здійснюється вищим навчальним закладом. На жаль, у змісті підготовки відсутня навчальна дисципліна, яка б знайомила студентів – майбутніх економістів – з вимогами систем безпеки корпоративної інформації, які реально існують на підприємствах і фірмах, у банках та організаціях. Таку дисципліну вивчають лише майбутні банківські службовці та фахівці із зовнішньоекономічної діяльності. Така ситуація є незрозумілою та невиправданою в умовах втрат комерційної інформації, що постійно зростають.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор. Різним аспектам захисту інформації в економічній діяльності надають увагу багато авторів (Г.А. Андрощук, Г.Г. Браїловській, М.С. Вертузаєв, Г.І. Зубок, Н.І. Реверчук, Л.Г. Стрельбицька, Г.П. Стрельбицький, М.І. Татарчук, Л.В. Чижевська, В.О. Хорошко, В.І. Ярочкін та інші). Зауважимо, що серед наукових робіт не виявлено досліджень, присвячених особливостям професійної підготовки економістів до роботи в корпоративній системі захисту інформації (КСЗІ). Це створює

суперечність між високим технічним потенціалом КСЗІ і непідготовленістю людського ресурсу. Аналіз публікацій в області педагогіки виявив, що подібними проблемами в Україні займався тільки О.С. Щербій [2].

Формулювання цілей статті (постановка завдання). Мета роботи – розкрити вимоги корпоративної системи захисту інформації до професійної діяльності майбутнього економіста.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Проведене дослідження виявило, що проблемі формування готовності майбутніх економістів до роботи в КСЗІ у вищій школі не приділяється належної уваги. Так, аналіз навчальних планів виявив відсутність відповідних курсів на всіх напрямах підготовки фахівців-економістів, окрім майбутніх банківських службовців, які вивчають курс «Безпека банківської діяльності».

Опитування студентів ВНЗ, які готують фахівців економічного напряму, показало, що вони: не можуть виділити із загального обсягу інформації корпоративну інформацію конфіденційного змісту; не здатні визначити вимоги КСЗІ до професійної діяльності фахівця; не готові виконати вимоги стосовно захисту і зберігання конфіденційної інформації. Таким чином, стан готовності майбутніх економістів до роботи в КСЗІ виявився недостатнім.

Між тим, «сфера інформаційної безпеки – найбільш динамічна галузь розвитку індустрії безпеки в цілому. … Чим активніше запроваджуються досягнення техніки та електронні розрахунки у наданні фінансових послуг, тим більш досконалою стає технологія вчинення злочинів з використанням електронних систем, а кількість таких злочинів постійно прогресує. *Вчиненню цих правопорушень сприяють особиста корислива зацікавленість окремих працівників банків, недбале ставлення їх до виконання своїх обов'язків, порушення існуючих правил і інструкцій*» (виділено мною – Я. Касярум) [1, с. 360].

Починаючи виконувати професійні обов'язки, молодий фахівець повинен розуміти, що проблема захисту і зберігання інформації, яка становить вагомий ресурс у організаціях, які займаються фінансовою, страховою, виробничою діяльністю, є дуже важливою. Жорстка конкуренція на ринку обумовлює необхідність збереження та захисту конфіденційної інформації, що є комерційною таємницею. Оскільки до використання даної інформації на різних рівнях доступу залучені співробітники компанії, то виникає й проблема формування готовності персоналу до збереження корпоративної інформації та її захисту. Науковці вважають потенційно небезпечними тих осіб, які не здатні виконувати вимоги режиму внутрішньої безпеки фірми [1, с. 407].

Як відомо, кожна КСЗІ є вразливою і, на думку фахівців із захисту інформації, практично неможливо створити абсолютно невразливої системи, тому що її суттєвим ресурсом є люди [3; 4].

Вважаємо, що існує й інший підхід до проблеми, а саме – формування у ВНЗ фахівця економічного профілю як компетентного користувача, здатного працювати в умовах КСЗІ. Недостатня підготовленість майбутніх економістів може бути подолана шляхом упровадження курсу «Безпека економічної інформації в інформаційних системах».

Насамперед студентів слід ознайомити з поняттями «конфіденційна інформація», «комерційна таємниця», «банківська таємниця». Як відомо, у змісті цієї інформації виділяються два складники: корпоративна й особистісна. Залежно від типу організації превалює певний тип корпоративної інформації: технологічна, виробнича, маркетингова, управлінська, організаційна. Ознайомившись з питанням теоретично, вони мають навчитися виокремлювати інформацію з обмеженим доступом в професійній діяльності. Комерційною таємницею слід вважати відомості про: функціонування виробництва; плани перепрофілювання виробництва; організацію управління; перспективні плани розвитку; відомості про перспективні ринки збуту, про джерела сировини й товари, про вигідних партнерів; звіти з фінансової діяльності фірми; кредитні договори з банками; договори про купівлю та продаж; потребу у кредитах чи сировині; кредитоспроможність і стан кредитування; ділових партнерів, у тому числі кредиторів; хід ділових перемовин; укладені контракти (договори, угоди); цінову політику; дані про конкурентів, їх слабкі та сильні боки; умови фінансової діяльності; технологічні ноу-хау; заходи, які здійснюються конкурентами; дані про потенційних партнерів, перевірка їх сумлінності; інформація про місце зберігання вантажів, час і маршрути їх перевезення; виявлення осіб, перспективних для вербування шляхом підкупу, шантажу або іншого методу; зв'язки та можливості керівництва; виявлення кола постійних відвідувачів; науково-технічні досягнення, якщо вони не захищені авторським чи патентним правом; структуру й організацію служби безпеки фірми; методи та засоби захисту інформації.

До змісту банківської таємниці входять: *фінансово-економічний стан банку; відомості про стан рахунків клієнтів; операції клієнта та здійснені ним угоди; відомості щодо комерційної діяльності клієнтів; комерційна інформація чи комерційна таємниця банку; системи безпеки банку та клієнтів; криптографічні коди захисту інформації; відомості про рівень допуску працівників до конфіденційної інформації;*

поіменний склад банку; стан матеріального забезпечення працівників банку.

Наступним кроком підготовки майбутніх економістів до роботи в умовах КСЗІ є ознайомлення їх із структурою, завданнями та вимогами системи безпеки інформації.

У системі захисту конфіденційної інформації (будь-то банківська або корпоративна комерційна таємниця) виділяють: *законодавчо-правову складову*, що представлена в законах України; *нормативну складову*, яка визначена керівництвом організації; *організаційну структуру* (спеціальні підрозділи або працівники, які забезпечують виконання політики безпеки) і *політику безпеки* [3]. Деякі науковці (П. Б. Хорєв) вносять користувачів до системи безпеки, аргументуючи це їхнім безпосереднім впливом на КСЗІ, інші (Л. Г. Стрельбицька) не поділяють цієї думки. Нормативна складова системи безпеки організації чи підприємства повинна включати: колективний договір, трудові контракти; інструкцію про порядок роботи з відомостями, що становлять комерційну таємницю; наказ про допуск працівників до відомостей, що становлять комерційну таємницю, зобов'язання працівника дотримуватися встановленого режиму захисту інформації [1, с. 406].

Структура системи безпеки організацій [4] визначається часткою конфіденційної інформації, яку потрібно захищати. Деякі організації мають незначну частину закритої інформації і тому обмежуються організаційними методами. Там, де інформації такого типу більше, створюють систему безпеки, але розраховують, щоб її вартість узгоджувалась з величиною втрат від витоку інформації. Фінансові організації передусім використовують фізичний захист приміщень, використовують стандартне комерційне програмне забезпечення для обробки інформації та управління доступом до локальної мережі. Значно менша увага приділяється застосуванню методів шифрування інформації та захисту телефонних ліній зв'язку. Найбільша ж доля інформації з обмеженим доступом (більше 50%) зосереджена в банках, тому і КСЗІ у них є найбільш високотехнологічними. Аналізуючи систему банківської безпеки в Україні, Л.Г. Стрельбицька так визначає її проблеми: «Саме проблема безпеки інформації є зараз найактуальнішою й найменш дослідженою. … Особливо актуальна порушена проблема в Україні. У західних банках програмне забезпечення розробляється конкретно під кожен банк, і автоматизована система обробки інформації банку є комерційною таємницею. В Україні поширені «стандартні» банківські пакети, інформація про які широко відома, що полегшує несанкціонований доступ у банківські комп'ютерні системи» [1, с. 362].

Вважаємо, що вже у вищому навчальному закладі майбутній економіст (банківський службовець, працівник страхової компанії, економіст фірми, бухгалтер, аудитор і інші) повинен у процесі професійної підготовки пройти початковий етап адаптації до умов професійної діяльності, повинен усвідомити суть вимог, які висуває до працівників КСЗІ, в якій існує конфіденційна комерційна інформація, що підлягає зберіганню та захисту. Найповнішими є вимоги банківської системи до своїх працівників, саме тому, на нашу думку, краще знайомити студентів з їх змістом.

«Кожен працівник підприємства, котрий працює з інформацією, що становить комерційну таємницю, зобов'язаний:

– знайомитися тільки з тими відомостями і документами, до яких він дістав доступ на підставі своїх службових обов'язків;

– знати, кому із співробітників дозволено працювати з відомостями, що становлять комерційну таємницю, і в якому обсязі ці відомості можуть бути доведені до цих працівників;

– працівник може знайомити представника сторонніх організацій з відомостями, що становлять комерційну таємницю, лише з письмового дозволу керівника структурного підрозділу;

– не розголошувати відомості, що становлять комерційну таємницю;

– не передавати третім особам і не розкривати публічно такі відомості без згоди керівника підприємства;

– виконувати вимоги наказів, інструкцій і положень із забезпечення збереження комерційної таємниці підприємства, що стосуються працівника;

– при спробі сторонніх осіб одержати від працівника відомості про комерційну таємницю негайно повідомити про це службову особу свого підприємства;

– зберігати комерційну таємницю тих підприємств, з якими встановлено ділові стосунки;

– при звільненні працівника всі носії комерційної таємниці підприємства (рукописи, чернетки, документи, креслення, друкарські стрічки, перфокарти, перфострічки, диски, роздрук на принтері (ксероксі), кіно-фото-негативи й позитиви, моделі, матеріали та інші відомості, що визначені як комерційна таємниця), які були в його розпорядженні у зв'язку з виконанням службових обов'язків під час роботи в банку, передати уповноваженій особі або до відповідного підрозділу підприємства;

– про втрату або нестачу носіїв комерційної таємниці (посвідчень, перепусток, ключів від режимних приміщень, сховищ, сейфів (металевих шаф), особистих печаток та про інші факти, які можуть призвести до розголошення комерційної таємниці підприємства, а також про причини та

умови можливого витікання відомостей, що становлять комерційну таємницю, негайно повідомити відповідну службову особу чи підрозділ підприємства» [1, с. 406-407].

Окрім загальних вимог стосовно збереження конфіденціальної інформації майбутній економіст повинен розуміти основи реалізації професійної діяльності в умовах КСЗІ. Як користувач з певним рівнем допуску до закритої інформації, як суб'єкт системи він обов'язково проходить етапи ідентифікації, аутентифікації й авторизації. Зважаючи на визначений політикою безпеки рівень доступу до ресурсів системи, його вхід і користування ресурсами системи обов'язково реєструється, протоколюється й контролюється в системному журналі. Так само контролюється й використання ресурсів мережі Інтернет. Можливості доступу користувача до закритої інформації регулюються за допомогою або паролів, або ключів. У КСЗІ використовуються ключі асиметричного шифрування, що генеруються адміністраторами захисту за допомогою спеціальних генераторів, та ключі симетричного шифрування, які використовуються для апаратного шифрування. В разі неправильного введення паролю (більше трьох спроб) робоче місце користувача блокується системою захисту, яка сприймає ці спроби як атаку на неї [3; 4].

Майбутній економіст повинен знати наступні правила попередження витоку конфіденційної інформації:

− потрібно знати нескладні правила створення паролю та своєчасно його оновлювати:

− інформація про ключі або паролі не повинна розголошуватися й надаватися іншим особам;

− ключі або паролі забороняється навіть тимчасово передавати іншим особам;

− систематично пароль і ключі оновлюються, тому потрібно їх своєчасно змінювати (за визначеним графіком);

− після завершення роботи та на час перерв на робочому місці не повинно залишатися жодної інформації, а екран монітора має бути виключений;

− потрібно своєчасно звільняти операційну пам'ять комп'ютера;

− передачу електронних банківських документів каналами зв'язку або електронною поштою співробітник має здійснювати лише в зашифрованому вигляді з обов'язковим підтвердженням про їх отримання;

− забороняється використовувати засоби захисту у внутрішніх платіжних системах банку, системах «клієнт-банк» та програмних комплексах, що знаходяться за межами системи автоматизації банку. При здійсненні операцій з виконання платежів і корегування рахунків цінність цієї інформації має тимчасовий характер і достатньо забезпечити захист платежу в момент його проведення.

Висновки з цього дослідження та перспективи подальших пошуків у даному напрямку. Для попередження халатності та навіть кіберзлочинності вважаємо важливим превентивну підготовку майбутніх економістів до професійної діяльності в умовах корпоративної системи захисту інформації. Вона дозволить проводити навчання персоналу організацій основам загальної безпеки й захисту інформації на новому рівні. Стрімкий розвиток інформаційних систем у економіці сприяв і розвитку систем інформаційної безпеки. Відомо, що із злочинною метою вперше комп'ютер було використано в м. Мінеаполісі (США, штат Міннесота) в 1966 р. [5]. З того часу стрімкими темпами відбувається зростання кіберзлочинності. Свій внесок до проблем витоку конфіденційної інформації дають й інсайдери, користувачі локальних інформаційних систем, причому більшість витоків інформації зумовлена їхньою недбалістю. Попередити розвиток цих негативних явищ можна за допомогою цілеспрямованого формування економіста як компетентного користувача корпоративних систем захисту інформації. Вважаємо, що впровадження спецкурсу «Безпека економічної інформації в інформаційних системах» буде сприяти вирішенню цієї проблеми.

Список джерел:

1. Стрельбицька, Л.М., Стрельбицький, М.П., Пжевський, В.К. Банківське безпекознавство [Текст] / Л.М.Стрельбицька, М.П.Стрельбицький, В.К.Пжевський. – К.: Кондор, 2006. – 600 с.
2. Щербій, О.С. Педагогічні умови формування морально-психологічної готовності курсантів спеціалізованих ВНЗ до професійної діяльності: [монографія] [Текст] / О.С. Щербій; Держ. служба спец. Зв'язку та захисту інформації України, Ін-т спец. Зв'язку та захисту інформації НТУУ «КПІ». – К.: Три К, 2011. – 254 с.
3. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах [Текст] / П.Б.Хорев – М.: Академия, 2005. – 256 с.
4. Татарчук, М.І. Корпоративні інформаційні системи: [навч. посібник] [Текст] / М.І. Татарчук. – К.: КНЕУ, 2005. – 290 с.
5. Компьютерные террористы: Новейшие технологии на службе преступного мира // Энциклопедия преступлений и катастроф / Автор-составитель Т.И. Ревяко. – Минск, 1997. – С. 34.