**ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ВІННИЦЬКИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО ТОРГОВЕЛЬНО-ЕКОНОМІЧНОГО УНІВЕРСИТЕТУ»
БІЛОЦЕРКІВСЬКИЙ ІНСТИТУТ НЕПЕРЕРВНОЇ ПРОФЕСІЙНОЇ
ОСВІТИ ДЗВО «УНІВЕРСИТЕТ МЕНЕДЖМЕНТУ ОСВІТИ»**

ПРОФЕСІЙНА КОМПЕТЕНТНІСТЬ ПЕДАГОГА В УМОВАХ ОНОВЛЕННЯ ЗМІСТУ ОСВІТИ ТА ВИМОГ РИНКУ ПРАЦІ
(з акцентом на особливості воєнного часу)

ЗБІРНИК МАТЕРІАЛІВ
VI Всеукраїнської
науково-практичної конференції

26 січня 2023 р.
м. Вінниця

УДК 371.122.1

Професійна компетентність педагога в умовах оновлення змісту освіти та вимог ринку праці (з акцентом на особливості воєнного часу. Матеріали VI Всеукраїнської науково-практичної конференції – Вінниця: ВСП «ВТЕФК ДТЕУ», ТОВ «Вінницька міська друкарня», 2023.-273 с.

У збірнику матеріалів конференції розглядаються питання:

1. Психолого-педагогічні аспекти в освітньому процесі закладів освіти в умовах воєнного стану.

2. Розвиток DIGITAL-технологій як чинник забезпечення організації освітнього процесу в умовах воєнного стану.

3. Протидія кіберзагрозам, цифрова грамотність та інформаційна гігієна викладачів та здобувачів в освітньому процесі.

4. Особливості роботи зі студентами у статусі тимчасово переміщених осіб.

5. Особливості профорієнтаційної роботи та організація вступної компанії в умовах воєнного стану.

6. Роль стейкголдерів у організації освітнього процесу закладів освіти.

За достовірність фактів, статистичної інформації, власних імен, цитат та інших відомостей, наданих у рукописах, відповідальність несуть автори публікацій.

Світлана ЯРЕМКО,
Лариса РАДЗІХОВСЬКА,
викладачі Вінницького торговельно-економічного інституту ДТЕУ

НАПРЯМКИ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

У сучасному світі інформація стає найдорожчим активом у житті людини та суспільства загалом. В епоху інформаційних технологій стає можливим майже миттєво отримувати інформацію, яка з'являється кожну секунду в різних куточках світу, зокрема щодо заключених торговельних угод, коливання валют і цінних паперів, запуску нових бізнес-проєктів та багато іншого. У зв'язку із цим, все більшої актуальності набуває питання захисту інформаційних ресурсів бізнес-структур засобами сучасних інформаційних технологій і систем. При цьому основною метою створення системи захисту інформації стає забезпечення надійного зберігання та ефективного використання інформації в діяльності бізнес-структур.

Проведемо аналітичний огляд сучасних аспектів захисту інформаційних ресурсів бізнес-структур та визначимо напрямки оптимізації існуючих методів та засобів забезпечення цілісності, доступності та конфіденційності інформації.

На початку розгляду суті та основних понять інформаційної безпеки варто зазначити, що вони з'явилося в кінці 80-х років. У працях німецького вченого Г. Одермана комплексно розглядалися проблеми безпеки, пов'язані з інформаційними загрозами. А у вітчизняній і зарубіжній пресі з кінця 1991 - початку 1992 року спостерігалась тенденція до відкритого дослідження проблеми інформаційної безпеки як окремого питання [2].

Цікавий погляд на поняття «інформаційна безпека» навів у своїх працях відомий український дослідник Калюжний Р.А., який вважає, що інформаційна безпека – це вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності, спеціальних правовідносин, які пов'язані зі створенням, зберіганням, поширенням і використанням інформації [5, с. 18].

Інформаційна безпека (ІБ) – це стан захищеності інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, зокрема, власникам і користувачам інформації та інфраструктури [4].

В Українській законодавчій базі термін «інформаційна безпека» наведено у Концепції національної програми інформатизації, затвердженої Законом України від 4 лютого 1998 року № 75/98, де «інформаційна безпека» - невід'ємна частина політичної, економічної, оборонної та інших складових національної безпеки. Об'єктами інформаційної безпеки є інформаційні

ресурси, телекомунікації, канали інформаційного обміну, функціонування телекомунікаційних мереж і систем та інші елементи інформаційної інфраструктури країни» [4].

З інформаційної точки зору суб'єкт бізнесу являє собою комплекс компонентів, пов'язаних між собою єдиною метою, структурними відносинами, технологіями інформаційного обміну. Зазначені компоненти в процесі функціонування суб'єкта можуть змінюватися, на них можуть впливати різного роду внутрішні і зовнішні чинники, які складно прогнозувати і оцінювати. Всі компоненти можна сформувати в чотири групи:

- персонал;
- технічні засоби інформатизації;
- програмне забезпечення;
- документи і вважати як об'єкти захисту інформації [3].

З цією метою суб'єкти, що мають потребу в підтвердженні юридичної вагомості переданого повідомлення, домовляються про прийняття деяких атрибутів інформації, що описують і здатність бути юридично значимою. Дана властивість інформації особливо актуальна в системах електронних платежів, де здійснюється операція з пересилання коштів.

Актуальність даної вимоги виникла завдяки появі таких понять, як електронні гроші та Internet-banking. Використання всесвітньої мережі та нових технологій супроводжується такими явищами, як низький рівень культури безпеки, збільшення онлайн користувачів і залежності від цифрової інфраструктури, поширення небажаного контенту, розвиток кібершахрайства, витоки інформації, втрата даних, несанкціонований доступ до інформації. кібервійни та кібертероризм набувають глобального характеру та вираженої динаміки, що ускладнює їх виявлення та можливості протидії [8].

Захист інформації на підприємстві є дуже важливим і цей аспект повинен бути обов'язковим при укладенні контракту компанією з її працівником, особливо якщо цей працівник займає керуючу посаду в компанії. Небезпека, в першу чергу, загрожує інформації, що зберігається в інформаційних системах підприємства. У цю систему входять програмне забезпечення автоматизованої системи, програми для виконання конкретних завдань компанії, програмні оболонки, текстові редактори, пакети програм, бази даних. Інформація може надходити по локальній мережі з пристрою введення, а саме з клавіатури, з зовнішнього середовища, а саме з мережі Інтернет, за системою SWIFT, від інших компаній. Щоб гарантувати безпеку інформаційної системи підприємства, необхідно наділення повноважень зареєстрованим користувачам, серед яких можуть бути як певні особи, так і організації. Ці користувачі можуть здійснювати тільки зумовлені дії з використанням інформаційних технологій [9].

Небезпека інформації на підприємстві виникає з певних джерел (рис 1.).

Основні переваги комплексної системи інформаційної безпеки - це всебічне охоплення слабких місць, захист як зовні, так і зсередини, гнучке поєднання необхідних програмно-технічних і організаційних заходів.

Рис. 1. Джерела небезпеки для інформації на підприємстві

Побудова такої системи передбачає не просто її складання зі спеціалізованих засобів від різних виробників, як з конструктора, а й реалізацію єдиної концепції інформаційної безпеки. Саме всебічний концептуальний аналіз ІС дозволяє потім виробити оптимальну політику забезпечення цієї безпеки.

Малий бізнес часто використовує в якості захисту безкоштовні антивіруси або рішення, призначені для домашніх користувачів, але коли компанія доростає до певного масштабу, їй потрібні інші, спеціалізовані рішення, щоб грамотно управляти захистом свого підприємства.

На даний час на ринку програмних продуктів є ціла низка програм для безпеки. При цьому ринок програмних продуктів постійно поповнюються і видозмінюються, а також з'являються абсолютно нові, що враховують досвід раніше створених.

Зрозуміло, що застосування технічних засобів захисту інформації в жодному разі не замінює собою спеціаліста, який контролює сигнали, отримані за допомогою відповідних пристроїв, у разі порушення рубежів захисту. В останні роки з'явилася можливість підійти до вивчення проблеми захисту підприємницької інформації комплексно, оскільки переважна більшість опублікованих робіт присвячена або конкретним системам захисту інформації, або її окремим аспектам [7].

Одну з головних ролей у забезпеченні інформаційної безпеки підприємств різних організаційно-правових форм (малих підприємств, науково-виробничих об'єднань, фінансово кредитних установ і т. д.) відіграють принципи організації системи захисту комерційної таємниці, методики комплексного контролю і перевірки захищеності інформації, якісний аналіз основних завдань захисту інформації [1].

На основі усього наведеного вище можна виділити ряд рекомендацій щодо організації заходів стосовно захисту підприємницької інформації: забезпечення розмежування доступу до інформації, що використовується в системі підприємства; обмеження доступу до інформації, що вважається комерційною таємницею; використання багаторівневої ідентифікації для доступу до засекреченої інформації її власником або уповноваженим ним органом; застосування комплексних заходів для контролю захищеності інформації, що є власністю підприємства.

Отже, забезпечення інформаційної безпеки бізнес-структур полягає у здійсненні постійного контролю за джерелами виникнення потенційних загроз (антропогенні, технологічні та стихійні джерела) та необхідності здійснювати захист інформації різними способами (захист програм від читання та копіювання, захист авторських прав на інформацію, захист від несанкціонованого доступу і запуску програм).

Захист інформації на основі системи інформаційної безпеки є найбільш поширеним варіантом організації останньої, інколи навіть тотожним самій безпеці. На даний час заходи захисту інформації поширюються на економічну, правову, кадрову, організаційно-управлінську, технічну сфери діяльності суб'єктів підприємництва. Сучасні системи захисту інформації досить складні, дорогі і не зовсім надійні, що потребує подальших заходів щодо їх удосконалення.

Список рекомендованих джерел:

1. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. М.: Издательство агентства «Яхтсмен», 2001. 76 с.
2. Закон України «Про концепцію національної програми інформатизації / Відомості Верховної Ради України, 1998, № 27-28.
3. Зубок М.І. Інформаційна безпека в підприємницькій діяльності: навч. посібник. К.: КНТЕУ, 2006. 115 с.
4. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки: навч. посібник. Вінниця: ВНТУ, 2006. 115 с.
5. Ліпкан В. А. Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник . К.: КНТ, 2006. 280 с.
6. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности . М.: Нолидж, 2001. 150 с.
7. Соснін А. С., Пригунов П. Я. Менеджмент безпеки підприємництва. К.: Європейський ун-т, 2002. 128 с.