УДК:378.016:004+004.239

С. О. ВОСКОБОЙНІКОВ
Бердянський державний педагогічний університет, Бердянськ
Інститут освітніх інженерно-педагогічних технологій

ТЕОРЕТИЧНІ ТА МЕТОДИЧНІ ОСНОВИ ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ У ПРОФЕСІЙНІЙ ПІДГОТОВЦІ МАЙБУТНІХ ІНЖЕНЕРІВ-ПЕДАГОГІВ

У статті опубліковано дослідження та науково-технічне обґрунтування теоретичних та методичних основ застосування криптографічних методів захисту інформації у професійній підготовці майбутніх інженерів-педагогів.

Ключові слова: *інформатизація, телекомунікаційні та інформаційні мережі, теоретичні та методичні основи криптографічних методів захисту інформації, криптографічний шифр, криптографічний алгоритм, технології побудови криптографічних алгоритмів, методики визначення стійкості криптографічних систем.*

Постановка проблеми. Розвиток сучасних комп'ютерних технологій, використання інформаційних мереж відкриває колосальні перспективи розвитку в усіх галузях освіти, науки, економіки та техніки. Постійне вдосконалення та розвиток існуючих мереж і комплексів спеціальних інформаційно-телекомунікаційних систем, розроблення сучасних вітчизняних засобів криптографічного та технічного захисту інформації, забезпечення безпеки державних та економічно-комерційніх інформаційних ресурсів в інформаційно-телекомунікаційних системах постає як актуальна науково-технічна проблема. Визначення загроз інформації, формування вихідних даних для оцінки можливостей технічних засобів усіх видів розвідки і їх небезпеки, виявлення потенційних каналів витоку інформації є першочерговими завданнями системи інформаційної безпеки підприємств, відомств, наукових центрів та науково-освітніх закладів, держави. Використання криптографічних методів захисту інформації є не новиною і розвиток технологій криптографічних методів захисту інформації зумовлює інформаційну безпеку даних, проведення фундаментальних та прикладних наукових досліджень, різних факторів і фізичних полів, технічних рішень і технологій, що можуть бути використані для ведення розвідувальної діяльності і несанкціонованого збору інформації, особливо відомостей, що становлять комерційно-економічну чи державну таємницю.

Вирішення проблеми інформаційної безпеки в Україні регламентують: Закон України «Про державну таємницю», Закон України «Про Національну програму інформатизації», Закон України «Про Концепцію Національної програми інформатизації», Закон України «Про електронні документи та електронний документообіг», Закон України «Про електронний цифровий підпис», Закон України «Про захист інформації в автоматизованих системах»

Проблеми впровадження вивчення сучасних видів та засобів захисту інформації у професійну підготовку майбутніх фахівців у сфері захисту інформації приділяють велику увагу сучасні вітчизняні та зарубіжні науковці: І. Берник, І. Громико, В. Кельтон, *Д. Леонов*, А. *Лоу*, В. Матвеєв, І. Медвєдовський, В. Носов, П. Орлов, П.Сем'янов, Ю.Харін та ін.

Потреба впровадження в педагогічний процес майбутніх інженерів- педагогів вивчення криптографічних методів захисту інформації як одного із сучасних видів захисту інформації є актуальною, оскільки підвищує іх майбутні професійні якості у галузі захисту інформації.

Аналіз останніх досліджень і публікацій. Бурхливий розвиток інформаційних технологій наприкінці XX ст. призвів до зростання відносної важливості окремих аспектів суспільного життя. Внаслідок інформаційної революції основною цінністю для суспільства взагалі й окремої людини зокрема, поступово стають інформаційні ресурси. Організація соціуму почала трансформуватися у напрямку перерозподілу реальної влади від традиційних структур до центрів управління інформаційними потоками, зросла впливовість засобів масової інформації (ЗМІ). Інформатизація та комп'ютеризація докорінно змінюють обличчя суспільства. За таких обставин забезпечення інформаційної безпеки поступово виходить на перший план у проблематиці національної безпеки[3,11]

Національна безпека істотно залежить від забезпечення інформаційної безпеки, й у ході технічного прогресу ця залежність буде зростати. Визначень інформаційної безпеки на сьогодні існує досить багато. Лише в нормативних документах і в науковій літературі їх налічується шістнадцять. Єдиної думки про те, що таке інформаційна безпека немає. І в цьому, на нашу думку, головна проблема стану захисту інформації. Ми постійно говоримо про те, що інформаційна безпека забезпечується на належному рівні, але як ми можемо казати про це напевне, коли ми не маємо єдиних правил про те, що ми захищаємо, як захищаємо і від чого. Проблем інформаційної безпеки безліч, як і проблем розвитку процесу інформатизації. У цій сфері необхідно вирішувати питання, пов'язані з визначенням природи різних видів інформаційних небезпек (загроз), механізмів їхнього впливу на об'єкти інформаційної безпеки, можливих наслідків цих впливів, шляхів і методів їх нейтралізації або зменшення. З цієї низки проблем найбільш вивченими є проблеми, пов'язані із захистом інформації. Що ж до питань захисту людини, людських спільнот, суспільства в цілому, то з погляду розробки методології, шляхів, форм і методів забезпечення інформаційної безпеки вони вивчені недостатньо [5,6,7].

Інформаційна безпека (Information Security) має три основні складові: конфіденційність, цілісність і доступність. Конфіденційність належить до захисту інформації від несанкціонованого доступу. Цілісність означає захист точності і повноти інформації і програмного забезпечення. Доступність – це забезпечення доступності інформації і основних послуг для користувача в потрібний для нього час.

Із зростанням науково-технічного прогресу буде зростати і важливість питання інформаційної безпеки громадянина, суспільства, держави. Тобто інформація стала чинником, який може призвести до значних технологічних аварій, військових конфліктів та поразок у них, дезорганізувати державне управління, фінансову систему, роботу наукових центрів, і чим вищий рівень інтелектуалізації та інформатизації суспільства, тим потрібнішою стає надійна інформаційна безпека, оскільки реалізація інтересів, людей та держав все більше здійснюється за допомогою інформатизації. Враховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися світогляд та мораль як окремих осіб, так і суспільства в цілому, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності та форм проявів сучасних методів скритого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які протирічать інтересам національної безпеки, вироблення механізмів протидії їм у всіх напрямах [8,9,10,12].

Отже, інформатизаційна безпека суспільства, держави характеризується ступенем їх захищеності, та, як наслідок, стійкістю головних сфер життєдіяльності у відношенні до небезпечних інформаційних впливів. Інформаційна безпека визначається здатністю нейтралізувати такі впливи.

Формулювання цілей статті. Мета дослідження – дослідити та науково-технічно обгрунтувати теоретичні та методичні основи застосування криптографічних методів захисту інформації при підготовці майбутніх спеціалістів галузі захисту інформації.

Виклад основного матеріалу дослідження. У зв'язку з інтенсивним розвитком інформатизації суспільства, що накладає певний відбиток на розвиток економіки, суттєво впливає на темпи науково-технічного прогресу, підвищення продуктивності праці і удосконалення соціально-економічних відносин, проблема захисту інформації, в цілому, стає більш значущою в забезпеченні безпеки розвинених держав.

Характерними рисами інформатизації є:

– проникнення інформаційних процесів у всі основні сфери діяльності держави, суспільства, соціальних, наукових, виробничих та інших колективів, а також індивідуумів і формування власників інформації, якими виступають юридичні (державні і недержавні структури) і фізичні особи;

– інтенсивне впровадження різноманітних засобів обчислювальної техніки і різних інформаційних технологій в багатогалузеву діяльність людства;

– суттєве зростання ефективності діяльності людства і одночасне зростання ступеню ризику нанесення шкоди в результаті виникнення т.зв. нештатних ситуацій внаслідок всезростаючих обсягів автоматизації різноманітних процесів на базі застосування засобів обчислювальної техніки;

– відносна новизна взаємовідносин, що виникають в процесі інформатизації.

Глобальна комп'ютеризація суспільства і розповсюдження інформаційно-обчислювальних мереж на великих географічних просторах породжують ряд суттєвих проблем, найбільш важливою з яких є захист інформації від витоку і порушення її цілісності. Висока концентрація інформації підвищує значущість шкоди у випадку викрадення або втрати. Відносна простота її отримання в окремих випадках і практична безкарність при різних несанкціонованих діях з нею, стимулювали процес становлення і розвитку "комп'ютерної злочинності". До цього процесу, як показує світовий досвід, залучені достатньо широкі кола, в які входять як окремі фізичні особи, так і представники державних структур.

Світові засоби масової інформації подають висновки аналізу спецслужб, що мають безпосереднє відношення до різних аспектів захисту інформації, про те, що до 80% всього обсягу шкоди, нанесеної незаконним отриманням і використанням інформації, відбувається саме через її витік технічними каналами.

Розвиток спеціальних інформаційно-телекомунікаційних систем на сучасному етапі розвитку суспільства, який характеризується впровадженням новітніх технологій і систем є однією з глобальних науково-технічних стратегій, а одним з важливих завдань є не лише забезпечення функціонування вже існуючих, але і впровадження нових, які б не поступалися світовим стандартам та відповідали велінню часу.

Важливим напрямком діяльності у сфері криптографічного та технічного захисту є наукова та науково-технічна діяльність, що зумовлено необхідністю:

– постійного вдосконалення та розвитку існуючих мереж і комплексів спеціальних інформаційно-телекомунікаційних систем, розроблення сучасних вітчизняних засобів криптографічного та технічного захисту інформації, забезпечення безпеки державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

– визначення загроз інформації, формування вихідних даних для оцінки можливостей технічних засобів розвідки і їх небезпеки, виявлення потенційних каналів витоку інформації.

Основу забезпечення інформаційної безпеки в інформаційно-телекомунікаційних системах складають криптографічні методи і засоби захисту інформації.

Історично криптографія використовувалася з однією метою: зберегти секрет. Навіть сама писемність була свого роду шифруванням (у Стародавньому Китаї тільки вищі верстви суспільства могли навчатися писемності), досвід застосування криптографії в Єгипті відноситься до 1900 року до н.е.: автор шифру користувався незвичайними ієрогліфами. Є й інші приклади: дощечки з Месопотамії, на яких зашифрована формула виготовлення керамічної глазурі (1500 рік до н.е.), єврейський шифр ATBASH (500-600 роки до н.е.), грецький «небесний лист» (486 рік до н.е.) і шифр простої підстановки Юлія Цезаря (50-60 рік до н.е.).

Основними завданнями, які вирішує криптографія є: забезпечення конфіденційності, цілісності, достовірності, юридичної значущості інформації, оперативності доступу до інформації, невідсліджуваність дій клієнта.

В основі криптографічних методів лежить поняття криптографічного перетворення інформації, вироблюваного на основі певних математичних законів, з метою виключити доступ до даної інформації сторонніх користувачів.Це криптографічне перетворення називається алгоритмом шифрування (шифром), під яким розуміється сімейство однозначно оборотних відображень множини відкритих повідомлень спільно з простором ключів в множину закритих повідомлень (криптограм). Де: ключ – це конкретний секретний стан деяких параметрів алгоритму, який задає однозначне перетворення відкритого тексту.

Апаратно — програмні засоби криптографічного захисту інформації (наприклад у системі захисту СЕМП) забезпечують автентифікацію адресата та відправника електронних документів і службових повідомлень, гарантують їх достовірність та цілісність у результаті неможливості підробки або заміни документів у шифрованому вигляді.Криптографічний захист інформації має охоплювати всі етапи обробки електронних документів, починаючи з часу їх створення до зберігання в архівах. Використання різних криптографічних алгоритмів на різних етапах обробки електронних документів дає змогу забезпечити безперервний захист інформації в інформаційній мережі, а також відокремлену обробку інформації стосовно різних завдань інформатизації.

Для забезпечення розв'язання завдань суворої автентифікації установ, підключених до інформаційної мережі, розроблено систему ідентифікації користувачів, яка є основою системи розподілу ключів криптографічного захисту.

Відповідні ідентифікатори ключів записуються в електронні картки, які є носіями ключової інформації для апаратного шифрування.

Для забезпечення захисту інформації від модифікації з одночасною суворою автентифікацією та безперервного захисту платіжної інформації та інших інформаційних задач з часу її формування система захисту СЕМП включає механізми формування перевірки ЕЦП на базі несиметричного алгоритму RSA.Для забезпечення конфіденційності інформація СЕМП, що циркулює в інформаційній мережі, має пройти обробку АРМ-НБУ або АРМ-СТП. Програмно-апаратний комплекс АРМ-НБУ є єдиним шлюзом до всіх задач файлового обміну інформацією Національного банку. Генерація ключової інформації для апаратури захисту, Її транспортування, контроль за Її обліком і використанням, контроль за використанням апаратури захисту, техніко-експлуатаційне обслуговування та ремонт апаратури захисту, а також сертифікація відкритих ключів покладаються лише на службу захисту інформації Національного банку.

Зміст професійної підготовки майбутніх фахівців з комп'ютерної безпеки, фахівців з організації та технології захисту інформації, фахівців із комплексного захисту об'єктів інформатизації, фахівців із комплексного забезпечення інформаційної

безпеки автоматизованих систем, фахівців із комп'ютерної безпеки визначається Державними освітніми стандартами вищої професійної освіти і відбирається з урахуванням принципів професійного спрямування, інтегративності, модульності, індивідуалізації і диференціації.

Впровадження методів, форм і засобів навчання, що підвищують ефективність підготовки фахівців, реалізується завдяки використанню проблемного, комп'ютерного, проектного навчання комп'ютерних дисциплін, дистанційного навчання в режимі реального часу, адаптивних технологій навчання, навчання за методом аналізу ситуацій у малих групах, застосуванню інформаційних технологій на практичних заняттях у процесі вивчення професійно-орієнтованих дисциплін, створенню і використанню у навчальному процесі електронних підручників, посібників, лекцій, тренажерів, технологій телеконференцій, Інтернет-форумів та комп'ютерного тестування.

Застосування криптографічних методів захисту інформації в структурі теоретичної і практичної підготовки майбутніх інженерів-педагогів є актуальним і значущим у формування професійних якостей майбутнього інженера-педагога та відповідності його фахової компетентності запитам сучасного розвитку суспільства.

Формування системи знань та умінь застосування криптографічних методів захисту інформації у майбутніх інженерів-педагогів здійснюється з використанням спеціальних технологій та методик, а саме: технологій побудови криптографічних алгоритмів та методик визначення стійкості криптографічних систем.

Висновки.

1. Основу забезпечення інформаційної безпеки в інформаційно-телекомунікаційних системах складають криптографічні методи і засоби захисту інформації.
2. Застосування криптографічних методів захисту інформації є одним з ефективних і науково і технічно обгрунтованим сучасним видом захисту інформації.
3. Застосування криптографічних методів захисту інформації в структурі теоретичної і практичної підготовки майбутніх інженерів-педагогів є актуальним і значущим у формування професійних якостей майбутнього інженера-педагога та відповідності його фахової компетентності запитам сучасного розвитку суспільства.

Перспективами подальших пошуків у напрямку досліджень є розробка технології формування системи знань і умінь застосування криптографічних методів захисту інформації при підготовці майбутніх спеціалістів галузі захисту інформації.

Список використаної літератури

1. *Бабичев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии. – М.: Горячая линия – Телеком, 2001 – 120 с.*
2. *Венбо Мао. Современная криптографія: теорія и практика.: Пер. с англ. – М.: Издательский дом «Вильямс», 2005 – 768 с.*
3. *Воробьёв С. Защита информации в персональных ЭВМ. – М.: Издательство «Мир», 1993 – 312 с.*
4. *Закон України «Про інформацію» //ВВР, 1992, № 48, ст. 650*
5. *Закон України «Про державну таємницю» //ВВР, 1994, №16, ст. 94.*
6. *Закон України «Про Національну програму інформатизації» //ВВР, 1998, № 27-28, ст. 181.*
7. *Закон України «Про Концепцію Національної програми інформа-тизації» // ВВР, 1998, № 27-28, ст. 182.*
8. *Закон України «Про електронні документи та електронний документообіг» // ВВР, 2003, № 36, ст. 275.*
9. *Закон України «Про електронний цифровий підпис» // ВВР, 2003, № 36, ст. 276.*
10. *Закон України «Про захист інформації в автоматизованих системах» // ВВР, 1994, № 31, ст.. 286.*

11. Защита информации в персональных ЭВМ. А. В Спесивцев, В. А. Вегнер и др. – М.: Радио и связь, 1993 – 193 с.

12. Ирвин Дж., Харль Д. Передача даннях в сетях: инженерный поход.: Пер. с англ. – СПб.: БХВ – Петербург, 2003 – 448 с.

С.О. Воскобойников
Бердянский государственный педагогический университет, Бердянск

ТЕОРЕТИЧЕСКИЕ И МЕТОДИЧЕСКИЕ ОСНОВЫ ПРИМЕНЕНИЯ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКЕ БУДУЩИХ ИНЖЕНЕРОВ-ПЕДАГОГОВ.

В статье опубликовано исследование и научно-техническое обоснование теоретических и методических основ применения криптографических методов защиты информации в профессиональной подготовке будущих инженеров-педагогов.

Ключевые слова: информатизация, телекоммуникационные и информационные сети, теоретические и методические основы криптографических методов защиты информации, криптографический шифр, криптографический алгоритм, технологии построения криптографических алгоритмов, методики определения стойкости криптографических систем.

S.O. Voskoboynikov
Berdyansk State Pedagogical University, Berdyansk

THEORETICAL AND METHODICAL BASES OF APPLICATION OF CRYPTOGRAPHIC METHODS OF PRIV IN PROFESSIONAL PREPARATION OF FUTURE ENGINEERS-TEACHERS.

In the article research and scientific and technical ground of theoretical and methodical bases of application of cryptographic methods of priv is published in professional preparation of future engineers-teachers. It is well-proven that application of cryptographic methods of priv is one of effective, scientifically and by the technically grounded modern type of priv.

Key words: informatization, telecommunication and informative networks, theoretical and methodical bases of cryptographic methods of priv, cryptographic code, cryptographic algorithm, technologies of construction of cryptographic algorithms, methods of determination of firmness of the cryptographic systems.