УДК 004.056.5+6(09)
DOI https://doi.org/10.32782/2663-5984.2025/1.51

Кондратьєв В.Ю.
Національний технічний університет
«Харківський політехнічний інститут»

РОЗВИТОК КІБЕРБЕЗПЕКИ У СВІТІ: ДРУГА ПОЛОВИНА XX СТОЛІТТЯ

Стаття розкриває еволюцію засобів захисту інформації, що відбулася в другій половині XX століття та продовжує формуватися й досі. Особливу увагу приділено ключовим подіям, інноваціям і технологіям, які суттєво вплинули на розвиток кібербезпеки. Відкриття у 1969 році ARPANET, який служив основою для сучасного Інтернету, започаткувало новий етап обробки, зберігання та передачі даних. Це спричинило потребу у створенні спеціальних механізмів захисту, таких як криптографічні алгоритми, зокрема DES та RSA, що стали переломними рішеннями в боротьбі з кіберзлочинністю й забезпеченні конфіденційності інформації. Розвиток персональних комп'ютерів у 1980-х роках і одночасне виникнення комп'ютерних вірусів підкреслили необхідність створення антивірусних програм і систем багаторівневого захисту, таких як Norton Antivirus і McAfee. Водночас фундаментальну роль почав відігравати людський фактор – виникла потреба у навчанні навичкам цифрової гігієни та кібербезпеки серед користувачів. У 1990-х роках масове поширення Інтернету привело до появи нових викликів у сфері кібербезпеки, адже загрози не обмежувалися локальними системами й стали глобальними. Це обумовило необхідність розробки та впровадження міжнародних стандартів, правових актів і механізмів співпраці. Значним кроком у цьому напрямі стало прийняття США Закону про комп'ютерне шахрайство та зловживання (CFAA), який встановив правові норми боротьби з кіберзлочинами. Розглянуто взаємозв'язок між глобалізацією, розвитком інформаційних технологій і збільшенням масштабів та складності загроз у новому тисячолітті. Відзначено важливість безперервного прогресу в технологіях, підвищення кваліфікації персоналу та міжнародної співпраці як необхідних складових успішної стратегії кібербезпеки. Таким чином, еволюція засобів інформаційного захисту демонструє важливість комплексного підходу, який передбачає використання технічних, організаційних і правових механізмів. Це особливо актуально в умовах сучасного інформаційного суспільства, де кібербезпека стає ключовою умовою ефективного функціонування економіки, бізнесу та соціальних інститутів.

Ключові слова: *кібербезпека, історія науки і техніки, Інтернет, інформаційні технології, захист даних, комп'ютерні віруси, підготовка кадрів.*

Постановка проблеми. Друга половина XX століття стала періодом, коли технологічний прогрес перевершив найсміливіші очікування. Поява перших цифрових обчислювальних машин, подальше впровадження персональних комп'ютерів і створення глобальних мереж, таких як ARPANET, назавжди змінили уявлення про обробку, зберігання і розповсюдження інформації. Проте цей поступ у технологічному розвитку супроводжувався виникненням нових загроз, які раніше не існували поза межами фізичного середовища [1, с. 14]. Інформація, що поступово ставала найціннішим ресурсом суспільства, перетворилася на ціль для зловмисників. Так виникло поняття кібербезпеки – цілісної системи методів і засобів, спрямованої на захист інформаційних ресурсів від несанкціонованого доступу, викрадення та знищення.

На початку 1950-х рр. інформаційні технології ще перебували на стадії становлення. Відсутність уніфікованого підходу до забезпечення безпеки робила інформаційні системи вразливими. Перші електронні обчислювальні машини, такі як ENIAC, були настільки громіздкими й обмеженими у використанні, що мали переважно спеціалізоване застосування. Однак завдяки впровадженню транзисторної технології вже з другої половини XX ст. комп'ютери стали компактнішими й ефективнішими, що зробило їх привабливим інструментом для автоматизації процесів. На цій стадії захист інформації базувався переважно на фізичному контролі доступу до обладнання. Питання безпеки ставали на перший план лише тоді, коли інформація почала передаватися між пристроями і мережами.

Аналіз останніх досліджень і публікацій. Історія розвитку кібербезпеки у світі є темою, що заслуговує на більш глибоке висвітлення та аналіз. Існуючі публікації, такі як «Події з історії кібербезпеки за 50 років» [2], «Найгучніші кібератаки в історії» [3] та інші блогові статті наводять важливі події та гучні кібератаки, але здебільшого зосереджені на конкретних інцидентах, а не на глобальному розвиткові кібербезпекових технологій та підходів на довгострокову перспективу. Праця Subramanian R. [4] розглядає ретроспективу кібербезпеки у Індії та наголошує на відкритості та свободі поширення інформації, а також піднімає питання втручання держави у внутрішні справи окремих громадян. Дослідження [5] виокремлює питання кібербезпеки у судовій справі та розглядає історію різних програм, що призвели до шахрайських дій. Автори статті «World of Cyber Security and Cybercrime» [6] надають детальну інформацію щодо кібербезпеки та кіберзлочинності. Вона включає типи кібербезпеки, необхідність кібербезпеки, проблеми кібербезпеки, її переваги та недоліки, історію кіберзлочинності, типи кіберзлочинності. Стаття Венгерської Н.С. та Сулейманова А.Н. [7] розглядають особливості кібербезпеки України в контексті глобальних викликів та міжнародного співробітництва з Великобританією. Автори звернули увагу на необхідність постійного оновлення технологічних засобів і стратегій для ефективного захисту інформації та інфраструктури. Описано основні результати та ефективність стратегій кібербезпеки України з 2016 по 2021 р.

Попри велику кількість публікацій, всі вони обмежені регіоном досліджень чи висвітлюють лише короткий проміжок часу у XXI ст. Таким чином, більш детальне вивчення історії кібербезпеки є актуальним і необхідним.

Постановка завдання. Встановити яким чином забезпечується захист інформації у світі, починаючи з другої половини XX ст.

Виклад основного матеріалу. Стрімкий розвиток комунікаційних систем у 1960-х рр., зокрема створення ARPANET у 1969 р., який вважається основою сучасного Інтернету, вивів обробку та зберігання інформації на новий рівень [8, с. 14]. ARPANET створювався як науково-дослідницька ініціатива, що мала забезпечити стійкість передавання даних навіть у разі пошкодження частини мережі. Цей проект був задуманий як військовий інструмент, здатний забезпечити безперебійний обмін інформацією в умовах надзвичайних ситуацій, таких як збройні конфлікти або техногенні катастрофи. Завдяки унікальній архітектурі, мережа могла забезпечити передачу даних навіть за умови великих структурних ушкоджень, що стало проривом у комунікаційних технологіях. Однак із самого початку з'явилися очевидні виклики щодо безпеки такої відкритої архітектури. Основною проблемою стала відсутність механізмів захисту, що призводило до ризику несанкціонованого доступу до ресурсів мережі. Протоколи, які використовувалися для комунікації, не враховували критично важливих аспектів: ідентифікацію користувачів, контроль доступу, а також шифрування переданих даних. Унаслідок цього ARPANET став об'єктом перших спроб кіберзломів і зловживань, які підкреслили необхідність розробки нових стандартів захисту інформації у мережах. Ці інциденти започаткували роботу над створенням безпечних інтернет-протоколів, а також стимулювали появу концепцій сучасної кібербезпеки

Саме в цей період розпочався перший етап становлення криптографії як засобу захисту інформації. Хоча криптографія здавна використовувалася для захисту секретних даних, перехід від механічних і електромеханічних шифрувальних машин до цифрових алгоритмів став проривом. Алгоритм Data Encryption Standard (DES), який з'явився у 1977 р. [9, с. 38], став першим глобально визнаним стандартом для шифрування даних у цивільних і військових системах. DES дозволяв використовувати 56-бітові ключі для шифрування даних, забезпечуючи захист інформації від випадкових зломів [10, с. 1]. Проте із подальшим розвитком обчислювальної техніки його слабкі сторони стали очевидними, що надихнуло на створення нових, ефективніших систем захисту.

У цьому ж періоді була створена ще одна технологія, яка назавжди змінила уявлення про захист даних: RSA. Представлений у 1978 р., алгоритм RSA базувався на принципах асиметричного шифрування [11, с. 982]. Він працював із двома ключами: один відкритий для шифрування даних і другий закритий для розшифрування. Така система, основана на математичних принципах, зокрема на складності факторизації великих чисел, забезпечувала надзвичайно високий рівень безпеки. Цей підхід забезпечував не тільки конфіденційність передачі інформації, але й її автентичність, дозволяючи ідентифікувати відправника даних і гарантувати, що повідомлення не було змінено під час передачі. Перехід до алгоритмів асиметричного шифрування став важливим етапом у забезпеченні безпеки елек-

тронних комунікацій. Він відкрив шлях до широкого використання цифрових підписів, які стали незамінними в сучасному цифровому світі, особливо для електронного документообігу, онлайн-транзакцій і забезпечення юридичної сили електронних документів.

У той же час питання людського фактора у забезпеченні кібербезпеки також набуло важливого значення. Багато інцидентів виявляли слабкі точки не тільки у самих технологіях, але і в людській поведінці. Цей період показав, що навіть найсучасніші системи можуть бути зламані через необережність, недостатні знання або недбалість користувачів. Як результат, у 1970-х рр. з'явилися перші концепції навчання і обізнаності у сфері кібербезпеки.

Продовженням ранніх експериментів у комунікаціях і захисті даних стало вдосконалення підходів до мережевої взаємодії та впровадження багаторівневих систем захисту. У 1980-х рр. вперше були реалізовані централізовані системи управління доступом, які дозволяли сегментувати права користувачів у корпоративних і державних мережах. Саме цей підхід зародив сучасну концепцію багатофакторної аутентифікації.

Період 1980-х рр. відзначився стрімким розвитком персональних комп'ютерів, завдяки чому інформаційні технології стали доступними не лише для великих організацій та урядів, а й для звичайних користувачів. Однак разом із цим розвитком почали масово виникати нові загрози, які стосувалися не лише крадіжки чи пошкодження даних, а й функціонування систем загалом. Комп'ютерні віруси стали одним із найбільш помітних явищ того часу. Elk Cloner, який з'явився в 1982 р., вважається одним із перших справжніх вірусів. Його створення показало, що системи можуть бути вразливими до програмного коду, розробленого для саботажу або маніпуляцій із програмним забезпеченням. Одночасно це стало стимулом для появи перших програм антивірусного захисту.

Важливим фактором було те, що на той час більшість користувачів володіли дуже низьким рівнем обізнаності про можливі ризики в інформаційному середовищі. Комп'ютерні системи сприймалися як щось надто складне, що не потребує додаткового захисту, окрім фізичного доступу до пристроїв. Разом із зростанням популярності дискет, які використовувалися для перенесення даних, середовище стало сприйнятливим до поширення шкідливих програм. Хакерські угруповання, які лише починали формуватися, використовували ці технології для несанкціонованого втручання в роботу систем.

Однією з ключових подій цього періоду стали широкомасштабні атаки, пов'язані з поширенням вірусів і хробаків. У 1988 р. стався інцидент, пов'язаний із черв'яком Морріса, який вивів із ладу значну частину мереж Інтернет у США [12]. Треба зазначити, що вартість збитків оцінювалася у мільйони доларів, а на відновлення роботи систем були потрібні тижні. Ця подія продемонструвала слабкі місця ранніх обчислювальних мереж і показав, що широкодоступні мережі можуть бути простими цілями для недобросовісної діяльності. Реакцією на такі інциденти стало створення перших центрів реагування на кіберінциденти, одним із яких став CERT (Computer Emergency Response Team). Ці організації стали прототипами сучасних систем управління ризиками, які й досі відіграють важливу роль у захисті критичної інформаційної інфраструктури.

У той самий час кібербезпека почала набувати значення і в корпоративному секторі. Компанії усвідомлювали, що витік конфіденційної інформації може спричинити не лише фінансові збитки, але й втратити репутацію. Це стало поштовхом для розробки систем захисту корпоративних мереж, адже більшість інформації зберігалася локально, без великих централізованих баз даних. У відповідь на зростання загроз, таких як троянські програми і хробаки, розробники почали впроваджувати брандмауери та програми для виявлення аномалій у поведінці систем. Брандмауери, які виникли наприкінці 1980-х, стали ефективним рішенням для фільтрації шкідливого трафіку і контролю доступу до системи. Їхня роль у захисті мереж значно зросла і знаходить застосування навіть сьогодні.

Антивірусні рішення поступово перейшли від простих сканерів до багатофункціональних систем захисту, які могли не лише виявляти відомі віруси на основі сигнатур, але й аналізувати поведінку програмного забезпечення. Це був період, коли компанії Symantec і McAfee стали піонерами у створенні комплексного програмного забезпечення для захисту інформації, прокладаючи шлях до сучасних антивірусних платформ [13].

Активізація хакерських атак та небезпечні програмні загрози сприяли розвитку правового регулювання у сфері інформаційної безпеки. На національному рівні багато країн почали приймати закони, які регулювали питання використання інформаційних систем, а також запроваджували покарання за кібератаки. У Сполучених Штатах

був прийнятий Закон про комп'ютерне шахрайство та зловживання Computer Fraud and Abuse Act (CFAA), який вперше встановив правові норми для запобігання кіберзлочинам і дозволив притягати до відповідальності винних осіб [14, с. 92].

У 1990-х рр. розпочалася ера масового поширення Інтернету, яка принесла нові виклики для кібербезпеки. Якщо раніше більшість загроз мали локальний характер і стосувалися переважно захисту даних на окремих комп'ютерах або в межах закритих мереж, то з появою Інтернету можливості для атак набули глобального масштабу. Хакери отримали доступ до мереж, у яких могли діяти без фізичної присутності, що значно ускладнило завдання виявлення й запобігання кіберзлочинам. Усі ці зміни зробили питання захисту інформації не тільки технічною, але й суспільною проблемою.

Цей період характеризувався появою перших масових атак, які привернули увагу глобальної спільноти на необхідність посилення та стандартизації кібербезпеки. Однією з найбільш відомих атак була так звана DoS-атака (Denial of Service), коли велика кількість запитів перевантажувала сервери, унеможливлюючи їхню нормальну роботу. Вперше такі атаки почали здійснюватися організовано в середині 1990-х рр. Відсутність належних захисних механізмів зробила сервери вразливими, що призвело до значних збитків для компаній і державних установ.

У відповідь на ці виклики було створено багаторівневі системи захисту, які дозволяли знижувати загрози і забезпечувати безперервність роботи систем. Концепція багаторівневого підходу полягала в тому, щоб застосовувати декілька шарів захисту з різними функціями. Один із рівнів зосереджувався на захисті мереж, забезпечуючи безпеку трафіку. Інші рівні охоплювали перевірку кінцевих пристроїв, ідентифікацію користувачів і шифрування даних. Цей період сприяв розвитку брандмауерів із новими функціями, що могли блокувати шкідливий трафік на основі сигнатур і поведінкових аналізів.

Зазначимо, що у 1990-х р. також відбулося активне створення міжнародних стандартів у сфері кіберзахисту. Стандарт ISO/IEC 27001 був впроваджений як глобальний підхід до управління безпекою інформації [15]. Він передбачав не лише технічний захист, але й управління ризиками, контроль доступу, навчання персоналу та регулярні аудити системи. Цей стандарт став обов'язковим для темпів сучасної цифрової економіки, оскільки дозволяв організаціям знижувати ймовірність кібератак і забезпечував довіру клієнтів. Крім цього, стандартизація зробила можливим міжнародне співробітництво, оскільки всі учасники використовували подібні підходи до безпеки.

Розвиток Інтернету також сприяв появі інструментів масового впливу через інформаційні мережі. Хакерські атаки почали застосовуватися не тільки для викрадення даних, але й для політичного та економічного тиску. Один із найбільш відомих прикладів демонстрації кіберзагроз на цей час – атака на інфраструктуру Інтернету Сполучених Штатів у 1997 р., яка продемонструвала, що навіть системи з високим рівнем захисту не можуть бути повністю безпечними. Такий характер атак змусив держави створювати окремі органи, які б відповідали за моніторинг і попередження загроз.

У корпоративному секторі компанії почали усвідомлювати переваги надійної кібербезпеки. Вони активно впроваджували системи платформового управління ризиками, які допомагали компаніям аналізувати вразливості їхніх систем. Такі платформи не тільки ідентифікували загрози, але й надавали рекомендації щодо їх вирішення, допомагаючи організаціям економити ресурси. У багатьох випадках ці технології були розроблені у співпраці між державними структурами та приватними компаніями, що відкрило нову сторінку у взаємодії бізнесу і держави для досягнення спільної мети – забезпечення безпеки цифрового світу.

Одночасно з розвитком систем захисту активізувалися й атаки, спрямовані на користувачів. Електронні листи з прикріпленими файлами стали одним із перших засобів поширення шкідливих програм. Велика частина інцидентів була безпосередньо пов'язана з людськими помилками, коли жертви самостійно відкривали небезпечні вкладення. Це призвело до необхідності запуску програм із навчання кібергігієни та свідомого використання мереж [16, с. 394]. Програми з обізнаності користувачів, які почали запроваджуватися у 1990-х рр., стали важливою складовою сучасних систем кіберзахисту.

Друга половина XX ст. стала періодом, коли кібербезпека почала переростати з вузькоспеціалізованого технічного питання у глобальне завдання, що торкалося кожного аспекту суспільного життя. Вхідна роль інформації та технологій у повсякденну, політичну, економічну й стратегічну діяльність зробила інформаційні системи критично важливими інфраструктурами. Відповідно, будь-які загрози чи втручання у роботу цих

систем стали сприйматися як серйозне порушення національної й приватної безпеки. Кіберпростір став не лише новою ареною для комунікації, але й точкою, де стикалися інтереси різних сторін: урядів, корпорацій, дослідників і злочинців.

Одним із найбільших уроків стало усвідомлення того, що жодна інформаційна система не може бути повністю захищеною. Це була особлива епоха, яка продемонструвала схильність технологій до розвитку не лише як інструментів прогресу, але й як нового типу вразливостей. Хакерські атаки, що проявилися наприкінці XX ст., дуже швидко перейшли з розряду одиничних експериментів до глобальних організованих злочинних кампаній. Основними мотивами кіберзлочинців були фінансовий зиск, саботаж і шпигунство, причому останні два аспекти особливо активно використовувалися як засоби політичного та військового тиску.

Одним із вирішальних моментів стало усвідомлення ролі людського фактору у кібербезпеці. Теоретичні ідеї про абсолютний контроль над даними були поставлені під сумнів, коли стало очевидно, що значна кількість інцидентів відбувається через недбалість, недостатню підготовку або помилки користувачів. Це спричинило запуск програм із навчання кібергігієни як на корпоративному, так і на індивідуальному рівнях. Людей почали навчати основам захисту даних, запобігання несанкціонованому доступу та розпізнаванню загроз [17, с. 286].

Важливим висновком цього періоду стало те, що технічні інструменти ефективно працюють лише в комбінації з юридичною та організаційною базою. Наприкінці XX століття багато держав ухвалили перші закони, що регулювали питання доступу до даних, покарання за комп'ютерні злочини та нормування цифрової поведінки. Особливо ефективним прикладом стало запровадження Закону про комп'ютерне шахрайство і зловживання у США. Цей закон встановив відповідальність за несанкціоноване використання інформаційних систем, захищаючи інтереси як приватних осіб, так і корпорацій. Подібні ініціативи підготували ґрунт для розвитку міжнародного співробітництва у сфері кібербезпеки.

Висновки. Починаючи з другої половини XX ст. разом із розвитком інформаційних технологій почали проявлятися і загрози безпеки передачі інформації. Таким чином, наприкінці XX ст. виявилася потреба в розробленні глобальних стандартів, що могли б забезпечити уніфікований підхід до оцінки ризиків і мінімізації загроз. Стандарти ISO/IEC 27001 стали одним із ключових досягнень цього періоду, пропонуючи системний підхід до управління інформаційною безпекою. Вони визначили найкращі практики захисту, які охоплювали всі рівні організації: від технічних засобів до політик і процедур. Цей підхід забезпечував не лише технологічний захист, але й управління ризиками, постійний моніторинг і навчання персоналу.

Крім суто технічних рішень, важливим аспектом розвитку кібербезпеки виявилась міжнародна співпраця. Інтернет став глобальним засобом комунікації, тому жодна країна не могла вирішувати проблеми у сфері кіберзахисту самостійно. З'явилися перші міжнародні домовленості, спрямовані на боротьбу з кіберзлочинністю та підтримку стабільності інформаційних систем. Одночасно уряди різних країн почали працювати над гармонізацією своїх законів задля досягнення спільної мети.

Успіхи цього періоду заклали основу модерної кібербезпеки, забезпечивши фундамент для подальшого розвитку захисту в цифровому середовищі XXI ст. Інструменти, методики та стандарти, розроблені у другій половині XX століття, залишаються актуальними навіть через десятиліття. Навіть новітні виклики, такі як розвиток штучного інтелекту чи Інтернету речей, базуються на принципах, створених у той час. Отже, основним завданням залишається необхідність балансування між технологічним прогресом і впровадженням ефективних механізмів захисту.

Список літератури:

1. Clarke R. A., Knake R. K. Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins Publishers, 2010.

2. Події з історії кібербезпеки за 50 років. URL: https://datami.ua/podiyi-z-istoriyi-kiberbezpeki-za-50-rokiv (дата звернення: 09.12.2024).

3. Найгучніші кібератаки в історії. URL: https://goit.global/ua/articles/kiberbezpeka-nayhuchnishi-kiberataky-v-istorii (дата звернення: 06.12.2024).

4. Subramanian R. Tracing India's (Cyber) Security History from Colonial Times to the Present: Has Anything Changed. IEEE Annals of the History of Computing, 2020, С. 99, DOI: 10.1109/MAHC.2020.3001215.

5. Zafri F. Ransomware Attacks in History of Cyber World. International Journal for Research in Applied Science and Engineering Technology, 2022, C. 39–43. DOI: 10.22214/ijraset.2022.39758.
6. Rachana Buch, Nirali Borad, Pooja Kalola. World of Cyber Security and Cybercrime. 2018, STM Journals Conference Proceedings.
7. Венгерська Н. С., Сулєйманова А. Н. Cyber Security Of Ukraine In The Context Of International Cooperation With Great Britain And Globalization Challenges. Вісник Запорізького національного університету. Економічні науки, 2024, DOI: 10.26661/2414-0287-2023-4-60-14.
8. Denning D. E. Information Warfare and Security. Addison-Wesley, 1999.
9. Levy S. Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age. Penguin Books, 2001.
10. FIPS 46-3, Data Encryption Standard (DES). 1999. URL: https://csrc.nist.gov/files/pubs/fips/46-3/final/docs/fips46-3.pdf (дата звернення: 10.11.2024).
11. Kahn D. The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner, 1967.
12. Fostering Growth in Professional Cyber Incident Management. 2000. URL: https://www.sei.cmu.edu/about/history-of-innovation-at-the-sei/display.cfm?customel_datapageid_40842=41019 (дата звернення: 25.10.2024).
13. The Story of McAfee: How the Security Giant Arrived at a Second IPO. 2020. URL: https://surl.li/fjtots (дата звернення: 08.12.2024).
14. Whitman M. E., Mattord H. J. Principles of Information Security. Cengage Learning, 2012.
15. International Standard ISO/IEC 27001:2022. 2022. URL: https://www.iso.org/standard/27001(дата звернення: 25.10.2024).
16. Медведенко Н. В., Медведенко С. В. Кібербезпека та кібергігієна як засоби запобігання втручанням в діяльність захисника чи представника особи. Юридичний науковий електронний журнал, № 10, 2023.
17. Mitnick K. D., Simon W. L. The Art of Deception: Controlling the Human Element of Security. Wiley, 2002.

Kondratiev V.Yu. THE DEVELOPMENT OF CYBERSECURITY WORLDWIDE: THE SECOND HALF OF THE 20TH CENTURY

The article explores the evolution of information protection tools that took place in the second half of the 20th century and continues to influence progress today. Particular attention is paid to key events, innovations, and technologies that significantly shaped the development of cybersecurity. The creation of ARPANET in 1969, which served as the foundation for the modern Internet, marked the beginning of a new phase in data processing, storage, and transmission. This led to the need for the development of specialized protection mechanisms, such as cryptographic algorithms, particularly DES and RSA, which became groundbreaking solutions in combating cybercrime and ensuring information confidentiality. The development of personal computers in the 1980s, alongside the emergence of computer viruses, highlighted the necessity of antivirus programs and multi-level defense systems, such as Norton Antivirus and McAfee. At the same time, the human factor began to play a fundamental role, creating the need for teaching digital hygiene and cybersecurity skills among users. In the 1990s, the widespread adoption of the Internet brought new challenges in the field of cybersecurity, as threats extended beyond local systems and became global. This underscored the need for the development and introduction of international standards, legal frameworks, and mechanisms of cooperation. A significant milestone in this direction was the adoption of the Computer Fraud and Abuse Act (CFAA) in the United States, which established legal measures to counter cybercrimes. The relationship between globalization, the development of information technologies, and the growing scale and complexity of threats in the new millennium is examined. The importance of continuous technological progress, staff training, and international cooperation forms the basis of a successful cybersecurity strategy. Thus, the evolution of information protection tools demonstrates the necessity of a comprehensive approach that incorporates technical, organizational, and legal mechanisms. This is especially relevant in the context of today's information society, where cybersecurity is a key condition for the effective functioning of the economy, business, and social institutions.

Key words: *cybersecurity, history of science and technology, Internet, information technologies, data protection, computer viruses, personnel training.*