Аннотация: В статье проанализированы основные направления развития современного информационного общества и представлена характеристика актуальных проблем, связанных с этим.

Ключевые слова: информационное общество, информатизация, информационное пространство.

Abstract: The article deals with analysis main ways of the development of modern information society and its issues.

Key words: information society, informatization, information space.

УДК 343.3

ЧЕРНУХІН Ігор Олександрович

ДОСВІД ФЕДЕРАТИВНОЇ РЕСПУБЛІКИ НІМЕЧЧИНИ В ПОБУДОВІ СИСТЕМИ ЗАХИСТУ ІНФРАСТРУКТУРИ ВІД КІБЕРНЕТИЧНИХ ЗАГРОЗ

Постановка проблеми. Стрімкий розвиток інформаційних технологій та їх проникнення в усі сфери життя зумовлює поступове переосмислення цінностей суспільства на інформаційні ресурси. Суспільство невпинно трансформується у напрямі перерозподілу влади від традиційних структур до центрів управління інформаційними потоками. Саме цим можемо пояснити зростання впливу засобів масової інформації (ЗМІ) та глобальних інформаційних мереж на суспільство. Інформатизація та комп'ютеризація докорінно змінюють його обличчя. Рівень проникнення інформаційних технологій та глобальних мереж у суспільство безпосередньо пов'язаний із рівнем розвитку країни. Саме тому Німеччина як одна із провідних країн світу (за абсолютною величиною валового внутрішнього продукту ФРН посідає 3 місце у світі за США і Японією), рівень інформатизації якої становить 80 %, значну увагу приділяє інформаційній сфері.

Глобалізація інформаційних відносин зумовлюють світову тенденцію до переведення протиправної діяльності у віртуальний простір. На сьогодні комп'ютерна злочинність чи, вживаючи західну термінологію, – кіберзлочинність, для якої не існує державних кордонів, загрожує не лише правам та майну громадян, а й посягає на національні інтереси та безпеку держав.

Протягом останніх трьох років окреслилась стійка тенденція збільшення проявів комп'ютерних атак на важливі об'єкти національних інфра-

структур іноземних країн (США, Австралія, Саудівська Аравія, Франція, Велика Британія, Іран), що призводило до завдання шкоди державам через спотворення важливої для них інформації, блокування виробничих процесів на об'єктах промисловості, житлово-комунального господарства, транспорту, енергетики.

Це свідчить про необхідність трансформації традиційної державної інформаційної політики провідних країн світу, яка переважно спрямована на захист інформації з обмеженим доступом (державної та службової таємниці), на забезпечення комплексної безпеки всіх об'єктів інформаційної інфраструктури, що використовуються для обробки, зберігання інформації (як державної таємниці, так і інших видів – персональних даних громадян), а також для управління технологічними процесами національних економік (промисловість, енергетика, транспорт, телекомунікації, об'єкти житлово-комунального господарства тощо).

Враховуючи, що такі загрози притаманні й Україні, слід зазначити про важливість вжиття для нашої країни аналогічних заходів, які мають враховувати результати наукових досліджень у цій сфері. Тому автор наголошує про важливість дослідження досвіду провідних країн світу у сфері побудови систем кібернетичного захисту, зокрема Федеративної Республіки Німеччини як ключової країни Європейського Союзу, інтеграційні прагнення до якого залишаються одним із головних пріоритетів зовнішньополітичного курсу України.

Аналіз останніх досліджень і публікацій. Міжнародний досвід забезпечення інформаційної безпеки досліджували у своїх працях І.Авдошин, А.Андрейчук, О.Архипов, В.Безногих, А.Жбанов, В.Крутов, Ю.Супрунов, В.Тиква. Вивчення проблеми організації захисту критичної інфраструктури від кібернетичних загроз на прикладі США та країн ЄС здійснювали О.Єрменчук, П.Скурський [1], В.Нідільніченко [2]. На окрему увагу заслуговує праця В.Біка, О.Климчука, В.Панченко та В.Петрова [3], в якій досліджено організаційно-правові засади побудови системи протидії кібернетичним загрозам у 6 країнах (як із високим, так і низьким рівнем кібернетичної міцності). Проте, ці праці не стосувалися питань забезпечення безпеки інформаційної інфраструктури ФРН. Окремі аспекти захисту в Німеччині інформації з обмеженим доступом, насамперед персональних даних, без дослідження проблеми організації захисту інфраструктури від кібернетичних загроз наведено у працях О.Матяша [4], О.Гореліхіної [5].

Отже, на системному рівні питання побудови захисту національної інфраструктури ФРН від кібернетичних загроз не досліджувалися.

Метою статті є дослідження ґенези державної політики ФРН у формуванні організаційно-правових засад захисту інфраструктури від кібернетичних загроз для подальшого врахування цього досвіду у вітчизняній сфері державної безпеки. Завданнями статті автор визначає: аналіз законодавства Німеччини у сфері організаційних основ захисту інформа-

ції, санкцій за їх порушення, термінології у сфері захисту кібернетичного простору, загроз та ризиків кібернетичній безпеці ФРН, визначення об'єктів інфраструктури, що потребують першочергового захисту, а також федеральних органів, до компетенції яких входить протидія таким загрозам.

Виклад основного матеріалу. Перші законодавчі кроки Федеральної влади Німеччини щодо захисту інформації відносяться до 70-х років минулого століття та пов'язані із захистом особи від посягань на недоторканість її приватного життя шляхом маніпулювання персональними даними. У 1977 році був прийнятий Закон ФРН "Про захист персональних даних", який у 1990 році набув нової редакції через возз'єднання ФРН та НДР в єдину німецьку державу, а також через поступове впровадження в німецьких структурах (федеральні, земельні, муніципальні органи, ЗМІ, приватні фірми тощо) автоматизованої обробки такої категорії інформації поруч із картотечною формою [5; 6]. У 1997 році у ФРН прийнято Закон "Про основи надання інформаційних та комунікаційних послуг", який регламентує вимоги захисту інформації лише в інформаційно-телекомунікаційних мережах загального користування [7]. Важливість захисту автоматизованих мереж технологічного управління об'єктів економіки, інших потенційно небезпечних об'єктів ФРН або так званої "критичної інфраструктури" (таку дефініцію вперше на правовому рівні увели в США у 1998 році) було визначено у Німеччині на законодавчому рівні в 2009 році. Так, Законом ФРН "Про посилення безпеки інформаційних систем" на Федеральне відомство безпеки інформаційних систем (BSI) ФРН покладено завдання попередження, реагування на інциденти, викликані кібернетичними загрозами, управління та координація сил та засобів із захисту критичної інформаційної інфраструктури, зокрема у взаємодії із приватним сектором [8].

У межах реалізації такого завдання BSI розроблено, а Федеральним Урядом у 2011 році затверджена Стратегія забезпечення кібернетичної безпеки ФРН (далі – Стратегія), яка є головним доктринальним документом ФРН із захисту інформаційної інфраструктури країни від кібернетичних атак. Концепція визначає низку дефініцій у галузі кібернетичної безпеки, кібернетичні загрози інформаційній інфраструктурі, об'єкти та суб'єкти посягання, а також організаційні засади протидії протиправним проявам, зокрема співробітництво із приватним сектором та міжнародними структурами [9].

У Стратегії визначено межі її регулювання – *кібернетичний простір,* який становить собою віртуальний простір, що містить у собі всі інформаційні мережі, які з'єднані між собою єдиними глобальними транспортними мережами (передусім інтернет). При цьому кіберпростір є відкритим для приєднання інших мереж передачі даних.

Автор зауважує, що німецький законодавець не включив до дефініції "кіберпростір" інформаційні мережі, які відокремлені від глобальних (так

звані "ізольовані мережі"). Таким чином, головною загрозою кібербезпеці ФРН фактично визначено кіберзлочинця, що за допомогою віддаленого несанкціонованого доступу (зокрема за межами Німеччини) здійснює протиправні дії з інформацією, на яку поширюється юрисдикція ФРН. Ця проблема має дискусійний характер, оскільки вчинення протиправних дій в ізольованих мережах можливе за необережністю персоналу самої мережі (упровадження вірусного флеш-накопичувача без перевірки), або за рахунок проникнення на об'єкт зловмисника. При цьому суспільно небезпечні наслідки від такого злочину можуть бути не менше ніж після віддаленої кібератаки хакерського угруповання. Прикладом цього може бути атака на інформаційну систему технологічного управління заводу із збагачення урану в Ісламській Республіці Іран у жовтні 2010 року, що відбулася через проникнення до мережі (була не підключена до інтернету) комп'ютерного вірусу StuxNet із флеш-накопичувача.

Кібернетичними загрозами національній інформаційній інфраструктурі ФРН визначено: витік інформації; порушення конфіденційності, цілісності та вірогідності інформації; блокування роботи об'єкта; перехоплення управління об'єктом; знищення об'єкта промисловості, транспорту, енергетики тощо. Такі загрози можуть бути реалізовані іноземними спецслужбами, терористичними організаціями, злочинними угрупованнями чи окремими особами-хакерами як із території Німеччині, так і ззовні.

Об'єктами, які можуть зазнати кібератак у Німеччині, визначені основні найважливіші інформаційні мережі, що забезпечують функціонування механізмів держави та суспільства, та які визначені як *національна критична інформаційна інфраструктура*. При цьому Німеччина у визначенні такої дефініції спиралась на досвід США та ЄС [10]. Так, німецький законодавець до національної критичної інформаційної інфраструктури відносить інформаційні мережі:

– енергетики;
– телекомунікацій;
– транспорту та дорожнього руху;
– охорони здоров'я;
– водозабезпечення;
– харчової промисловості;
– фінансової сфери та страхування;
– державного управління;
– засобів масової інформації й культури.

Автор зауважує, що окрему увагу в Стратегії присвячено другому та восьмому сектору національної критичної інформаструктури (інформаційним мережам загального користування та державного сектору).

Інформаційні мережі загального користування. Державна політика німецького Уряду із забезпечення безпеки мереж загального користування спрямована на забезпечення умов:

– безпечної інтернет-торгівлі в інтересах суб'єктів господарювання Німеччини;

– захисту персональних даних громадян ФРН у зв'язку із їх автоматизованою обробкою у мережах банків, пошти, комунальних служб, телекомунікацій тощо;

– захисту особистої інформації громадян під час її обміну засобами електронної пошти.

Забезпечення безпеки інтернет-торгівлі в інтересах суб'єктів господарювання Німеччини здійснюється за допомогою впровадження системи *електронного цифрового підпису* – виду електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача.

Державна політика із захисту персональних даних громадян ФРН у зв'язку із їх автоматизованою обробкою у мережах державних та комерційних структур регламентована Федеральними законами [6; 7] та базується на таких принципах:

обов'язкове віднесення персональних даних до інформації з обмеженим доступом;

надання персональних даних третім особам винятково за згодою власника персональних даних;

реєстрація баз персональних даних у секретаріаті уповноваженого Федерального Уряду з питань захисту персональних даних.

Крім того, особливу увагу у напрямі забезпечення захисту інформаційних систем займає захист особистої інформації громадян під час її обміну засобами електронної пошти. Стратегією визначено впровадження цільових пільг і державної підтримки німецьким розробникам сертифікованих засобів захисту інформації, що призначені для масового використання.

Інформаційні мережі державного сектору. Забезпечення захисту державної інформації є одним із головних завдань із забезпечення інформаційної безпеки Німеччини. Так, основними загрозами державному сектору у цій сфері є:

порушення конфіденційності, цілісності та доступності державної таємниці ФРН, що циркулює в інформаційних системах державних структур;

порушення цілісності та доступності відкритої державної інформації на офіційних інтернет-сайтах федеральних та земельних владних структур.

Із метою нейтралізації цих загроз Стратегією кібербезпеки ФРН передбачено:

– розробку та впровадження інформаційних систем для потреб держави здійснювати з урахуванням реальних та потенційних ризиків державній інформації у цих системах, зокрема враховуючи розвиток світових інформаційних технологій;

– створення загальної інформаційної мережі федеральних структур ("Netze des Bundes") із єдиним центром керування та контролю за захистом інформації;

– створення висококваліфікованих служб захисту інформації в державних структурах із можливістю обміну співробітниками між Федеральними відомствами;

– співробітництво із іншими країнами, передусім у межах системи CERT (команда реагування на надзвичайні події в інформаційних мережах) в питаннях оперативного реагування на кібератаки та мінімізації негативних наслідків.

Не менш важливими залишаються й *організаційні аспекти* протидії кіберзагрозам та реалізації основних положень Стратегії.

На думку автора реалізація ефективної державної політики із зміцнення кібербезпеки не можлива без побудови нової, або оптимізації існуючої системи державних органів, до компетенції яких входить забезпечення інформаційної безпеки. Так, загальносвітовий досвід протидії цим загрозам (передусім США) свідчить про побудову у провідних країнах *загальнодержавних систем протидії кіберзлочинності з єдиним координуючим органом*, які здатні в короткий проміжок часу акумулювати сили та засоби різних державних і недержавних органів для протидії та нейтралізації кібератак [3].

При цьому такі системи підпорядковуються главі виконавчої влади та, як правило, містять такі складові: *1) військова* – для здійснення розвідувальних та оборонних операцій в інтересах збройних сил; *2) захист так званої "критичної інфраструктури"* – для захисту, зокрема від терористичних посягань, інформаційно-телекомунікаційних систем органів державної влади, місцевого самоврядування, стратегічно важливих для держави підприємств, енергогенеруючих об'єктів, об'єктів транспорту, водо-, електро-, тепло- і газопостачання, життєзабезпечення та підвищеної небезпеки; *3) правоохоронна* – для запобігання, виявлення, припинення та розслідування комп'ютерних правопорушень, притягнення зловмисників до відповідальності.

Аналогічні підходи знайшли відображення і в Стратегії кібербезпеки Німеччини. Так, для оптимізації оперативного співробітництва між усіма державними установами й поліпшення координації заходів із захисту інформації, протидії кібератакам в ФРН створено *Національний центр кіберзахисту* (Nationales Cyber-Abwehrzentrum – NCAZ). Центр функціонує у сфері управління Федерального відомства захисту інформаційних систем (BSI, формує вимоги із захисту інформації в інформаційних системах держави) при безпосередній участі співробітників Федерального відомства захисту конституційного ладу (BfV, здійснює оперативно-розшукові заходи з виявлення кіберзлочинців) та Федерального відомства цивільного захисту й допомоги при стихійних лихах (BBK, вживає заходи щодо усунення суспільно небезпечних наслідків реалізації кібератак) [11].

Національний центр кіберзахисту підпорядковується Державному секретарю Міністерства внутрішніх справ ФРН та відповідно до законодавства ФРН має співпрацювати з Федеральним відомством карного розшуку (BKA, розслідує кримінальні справи у сфері порушень законодавства з охорони інформації), федеральної поліції (BPol), митниці (ZKA), Федеральної служби розвідки (BND), Бундесвером.

Єдина система має виконувати такі основні завдання:

– моніторинг інформаційних систем на предмет уразливості до кібератак;

– координація дії елементів Єдиної системи із блокування спроб реа-

лізації кібератак; ідентифікація та пошук ініціаторів кібератак;

– вжиття заходів із локалізації шкоди, викликаної зловмисними діями;

– розслідування комп'ютерних злочинів; встановлення вимог із захисту інформації в інформаційних мережах та надання відповідних рекомендацій; здійснення міжнародної взаємодії з питань протидії кіберзагрозам.

Крім побудови Національного центру Стратегією кібербезпеки передбачено також створення вищої дорадчо-консультативної структури – *Національної ради кібербезпеки,* головним завданням якої є розроблення пропозицій із вироблення стратегії державної політики та контроль виконання рішень керівництва держави у сфері протидії кіберзагрозам.

У складі Ради: Державні секретарі бюро Канцлера, Федеральних міністерств (закордонних справ, внутрішніх справ, оборони, економіки й технологій, юстиції, фінансів, освіти й науки), а також представники Федеральних земель.

Ця організаційна схема (рис. 1) становить собою так звану "базову структуру". Водночас її функціонування шляхом взаємодії між собою структурних елементів неефективне. Тому державна політика ФРН у сфері протидії кіберзагрозам передбачає два напрями співробітництва.

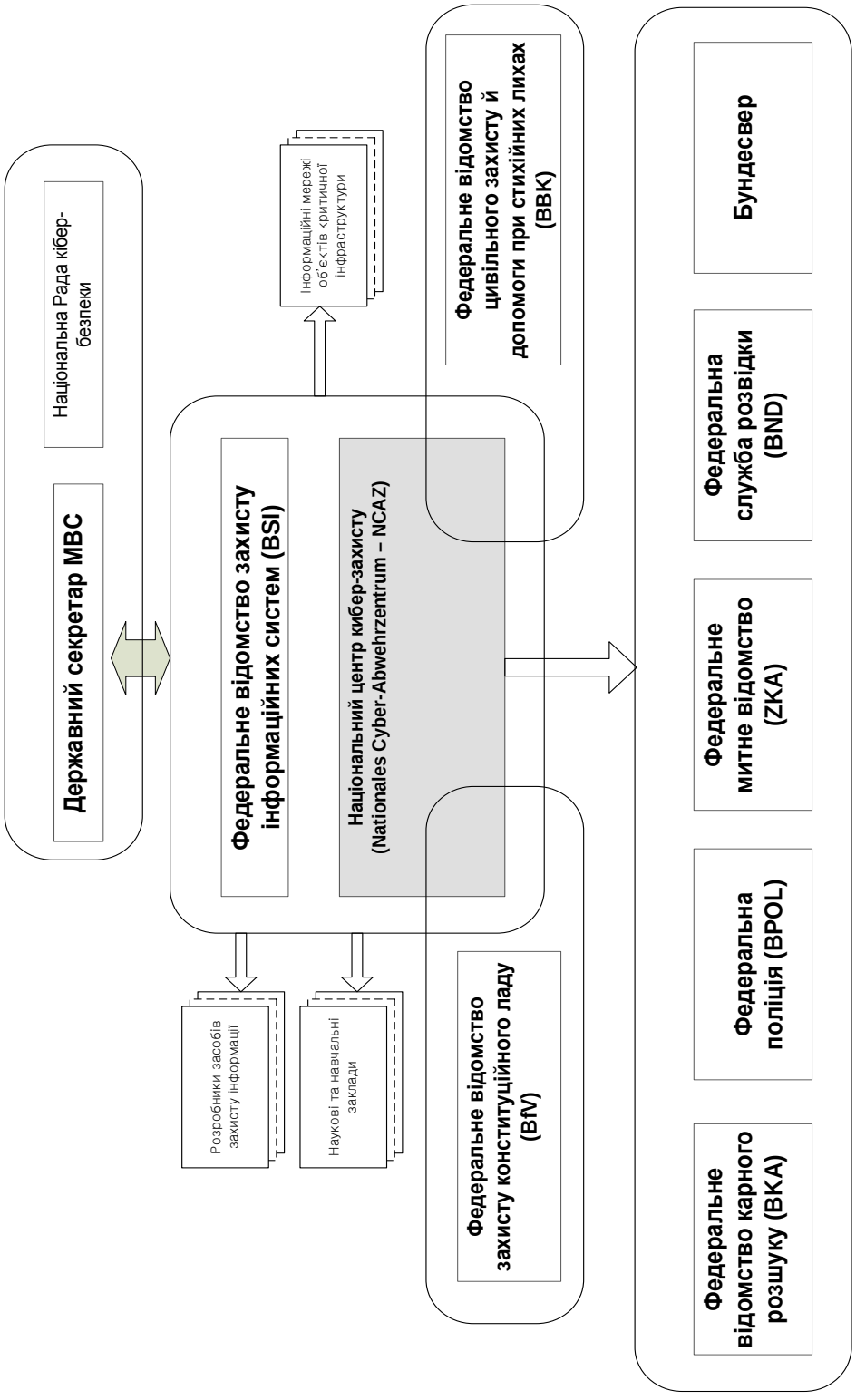

Рис. 1. Єдина Федеральна система забезпечення кібербезпеки

Так, кримінологічний аналіз проявів кіберзлочинності свідчить, що серед усіх мотивів, які викликають в особи рішучість несанкціонованого втручання в роботу інформаційних систем, понад 50 % становить *фінансова зацікавленість*. Тобто, інакше кажучи, понад половини кібератак спрямована проти інформаційних систем фінансово-банківської сфери. Більшість такого сегмента німецького ринку становлять приватні структури. Не виняток і знаходження у приватній власності й окремих об'єктів "критичної інфраструктури", яку Федеральний уряд визначив як пріоритет захисту від кіберзагроз.

Це зумовлює *перший напрям* співробітництва наведених вище державних структур із приватним сектором Німеччини, який співробітничає із:

– власниками об'єктів національної критичної інформаційної інфраструктури з метою протидії проведенню кібератак проти їх інформаційних систем;

– розробниками засобів захисту інформації із метою впровадження національних стандартів та надійних засобів захисту інформаційної інфраструктури;

– навчальними та науковими закладами для забезпечення висококваліфікованих кадрів Національної системи кібербезпеки.

Крім того, Федеральний уряд, акцентуючи увагу на інтернаціональному характері кіберзагроз, що передбачає проникнення в реальному масштабі часу до інформаційних мереж із будь-якої країни світу, у Стратегії кібербезпеки ФРН наголошує на необхідності взаємодії з іншими країнами у питаннях протидії таким загрозам. Так, *другий напрям* співробітництва передбачає взаємодію:

на рівні Європейського Союзу (ЄС) у межах виконання Плану спільних дій для захисту важливих інформаційних інфраструктур, виступаючи за розширення повноважень Європейського агентства мережевої та інформаційної безпеки (ENISA);

у межах НАТО, який є наріжним каменем трансатлантичної безпеки, що передбачає розробку та прийняття єдиних стандартів безпеки, вимоги яких держави-члени Північно-Атлантичного Альянсу можуть добровільно прийняти для захисту цивільного сегмента критичної інфраструктури;

з іншими міжнародними організаціями (G8, ООН, ОБСЄ, Рада Європи), виступаючи за розробку та прийняття міжнародного Кодексу поводження держав у світовому кіберпросторі;

із країнами, що розвиваються, шляхом надання наукової, технологічної та фінансової допомоги для подолання ризиків цих країн в інформаційній безпеці, та, як наслідок, унеможливлення здійснення кібератак із їх території на інформаційну інфраструктуру Німеччини.

Вважаємо, що дослідження досвіду ФРН із захисту інформаційної інфраструктури від кібернетичних загроз не слід обмежувати лише аналізом доктринальних нормативно-правових актів. Не менш важливим залишається вивчення й німецького законодавства, що регламентує відповідальність, насамперед кримінальну, оскільки більшість протиправних проявів у сфері інформаційної

безпеки за вітчизняним законодавством є злочинами [12].

Нормативним документом законодавства Німеччини, що визначає, які суспільно небезпечні діяння є злочинами та які покарання застосовуються до осіб, є Кримінальний закон ФРН (StGB) [13].

Із кримінально-правового погляду під кіберзлочином треба розуміти передбачені кримінальним законом суспільно небезпечні дії, в яких об'єктом злочину є інформація, оброблена інформаційною системою, або самі інформаційні та телекомунікаційні системи.

Аналіз Кримінального закону ФРН до злочинів у сфері кібербезпеки дає змогу віднести: антиконституційний саботаж (§ 88), порушення конфіденційності розмови (§ 201), порушення таємниці листування (§ 202), порушення таємниці поштової й телекомунікаційної таємниці (§ 206), комп'ютерне шахрайство (§ 263a), зміна даних (§ 303a), комп'ютерний саботаж (§ 303b), втручання в роботу телекомунікаційних установок (§ 317).

Об'єктивна сторона цих злочинів (зовнішня сторона діяння, яка виражається у вчиненні передбаченого законам діяння) передбачає такі протиправні діяння: виведення із ладу телекомунікаційного обладнання; застосування шкідливого обладнання та програмного забезпечення; перехоплення приватних та службових розмов, телекомунікаційної кореспонденції за допомогою технічних засобів; розголошення змісту приватних та службових розмов, телекомунікаційної кореспонденції; несанкціоновані дії з комп'ютерною інформацією.

У цілому кримінальне законодавство Німеччини дозволяє притягнути до відповідальності винних осіб, які вчинили кіберправопорушення із використанням новітніх технологій.

Порівняльний аналіз кримінальних законів ФРН та України (таблиця 1) свідчить про тотожність визначення злочинами суспільно небезпечних діянь у сфері кіберпростору.

Водночас, якщо українське законодавство визначає окремий розділ 16 Кримінального кодексу України, що об'єднує всі злочини проти інформаційних та телекомунікаційних систем (злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку), у Німеччині такі злочини не виокремленні в єдиний розділ, а присутні в розділах про посягання на державність, права и власність громадян. Таким чином, німецьке кримінальне законодавство визначає застосування інформаційних технологій у протиправних цілях (кібернетичні атаки) як спосіб та засіб для вчинення наведених вище кримінально караних діянь.

Таблиця 1

Кримінальний кодекс ФРН	**Кримінальний кодекс України**
§ 88. Антиконституційний саботаж (1) Хто, як організатор або підбурювач, не діючи із групою або для неї,	**Стаття 113. Диверсія** Вчинення з метою ослаблення держави вибухів, підпалів або інших дій,

Кримінальний кодекс ФРН	**Кримінальний кодекс України**
поодинці навмисне сприяє тому, щоб у сфері дії цього закону своїми шкідницькими діями повністю або частково вивести із ладу або унеможливити використання за призначенням … 2. *телекомунікаційного обладнання*, що використовується у суспільних цілях, … карається позбавленням волі на строк до п'яти років або штрафом. (2) Замах карний.	спрямованих на масове знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, на зруйнування або пошкодження *об'єктів, які мають важливе народногосподарське чи оборонне значення,* а також вчинення з тією самою метою дій, спрямованих на радіоактивне забруднення, масове отруєння, поширення епідемій, епізоотій чи епіфітотій, - карається позбавленням волі на строк від восьми до п'ятнадцяти років.
§ 201. Порушення конфіденційності розмови (1) Позбавленням волі на строк до трьох років або штрафом карається той, хто незаконно - записує на магнітофон конфіденційну, не призначену для інших осіб, інформацію іншої особи або - використовує зроблену в такий спосіб запис або розголошує її третій особі. (2) Так само карається той, хто незаконно - за допомогою підслуховувального пристрою отримує конфіденційну, не призначену для нього, інформацію або - робить доступною іншим особам записану (абз. 1) або підслухану (абз. 2) конфіденційну інформацію іншої особи, передаючи її дослівно або її загальний контекст. Діяння, зазначене в пропозиції 2, карається тільки в тому випадку, якщо доведена до відома громадськості конфіденційна інформація може завдати шкоди законним інтересам іншої особи. Діяння не є протиправним, якщо повідомлення такої інформації громадсь-	**Стаття 163. Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер** 1. Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер, - караються штрафом від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі до трьох років. 2. Ті самі дії, вчинені щодо державних чи громадських діячів або вчинені службовою особою, *або з використанням спеціальних засобів, призначених для негласного зняття інформації,* - караються позбавленням волі на строк від трьох до семи років. **Стаття 359. Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації** 1. Незаконне придбання або збут спеціальних технічних засобів негласно-

Кримінальний кодекс ФРН	**Кримінальний кодекс України**
кості здійснюється з урахуванням переваги в цьому випадку інтересів суспільства. (3) Позбавленням волі на строк до п'яти років або штрафом карається той, хто, будучи посадовою особою, або особою, спеціально уповноваженим на виконання публічної служби, порушує конфіденційність інформації (абз. 1 і 2). (4) Замах карний. (5) Записувальний або підслуховувальний пристрій, який використовувався правопорушником, може підлягати конфіскації. **§ 202. Порушення таємниці листування** (1) Хто незаконно … 2. знайомиться із змістом запечатаного листа, не розкриваючи його*, за допомогою технічного засобу*, карається позбавленням волі на строк до одного року або штрафом, якщо в діянні відсутні ознаки злочину § 206. (3) За змістом абз. 1 і 2 до документа прирівнюється зображення різного роду.	го отримання інформації, а також *незаконне їх використання* - караються штрафом від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до чотирьох років, або позбавленням волі на той самий строк. … 3. Дії, передбачені частиною першою або другою цієї статті, вчинені організованою групою або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам чи інтересам окремих громадян, державним чи громадським інтересам або інтересам окремих юридичних осіб, - караються позбавленням волі на строк від семи до десяти років.
§ 206. Порушення таємниці поштової й телекомунікаційної таємниці (1) Хто незаконно передає іншій особі відомості про факти, які становлять поштову й телекомунікаційну таємницю, і які стали відомі йому під час виконання службових обов'язків на підприємстві зв'язку, карається позбавленням волі на строк до п'яти років або штрафом. (2) Так само карається власник або службовець підприємства, зазначеного в абз. 1, який незаконно - здійснив доступ до змісту послання,	**Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї** 1. Несанкціоновані зміна, знищення або блокування інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або

Кримінальний кодекс ФРН	**Кримінальний кодекс України**
що було довірено такому підприємству для передачі, зокрема за допомогою технічних засобів, - приховує послання, довірене такому підприємству для його передачі, або - дозволяє робити або сприяє здійсненню дій, зазначених в абз. 1 або в № 1, або 2. (3) Абзаци 1 і 2 застосовуються і до осіб, які - виконують обов'язки контролю за діяльністю підприємства, зазначеним в абз. 1, - виконують обов'язки, покладені на них таким підприємством за дорученням (договором), - здійснюють виготовлення устаткування для такого підприємства, або виконують інші роботи для нього. (5) До поштової таємниці відносяться детальні відомості про поштовий обіг певних осіб, а також зміст поштових відправлень. До телекомунікаційної таємниці відносяться зміст телекомунікаційних повідомлень, відомості про трафік, його суб'єкти, зокрема щодо з'єднань, що не відбулися.	зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, - караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років із конфіскацією програмних або технічних засобів, за допомогою яких було вчинено несанкціоновані зміна, знищення або блокування інформації, які є власністю винної особи. 2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, - караються позбавленням волі на строк до трьох років із позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи.
§ 263a. Комп'ютерне шахрайство (1) Хто діє з метою одержання для себе або третьої особи протиправної майнової вигоди й цим завдає шкоди майну іншої особи тим, що він впливає на результат обробки даних ЕОМ, встановлюючи протиправні програми, використовуючи недостовірні або неповні дані, несанкціоновано застосовуючи дані або впливаючи на такий процес яким-небудь іншим неправомочним впливом, карається позбав-	**Стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут** 1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин

Кримінальний кодекс ФРН	**Кримінальний кодекс України**
ленням волі до п'яти років або штрафом.	(комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, - караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк, з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.
§ 303a. Зміна даних (1) Хто протиправно *знищує, робить непридатними до використання або змінює дані* (§ 202a, абз. 2), карається позбавленням волі на строк до двох років або штрафом. (2) Замах карний.	**Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку** 1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що *призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації*, - карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено не-
§ 303b. Комп'ютерний саботаж (1) Хто *порушує обробку даних*, які мають істотне значення для іншого підприємства, установи, організацій або державного органу таким чином, що він - вчинює діяння, зазначене в § 303a, абз. 1, або - знищує, пошкоджує, робить непридатним устаткування для обробки даних або носій даних, карається позбавленням волі на строк до п'яти років або штрафом. (2) Замах карний.	

Кримінальний кодекс ФРН	**Кримінальний кодекс України**
	санкціоноване втручання, які є власністю винної особи.
§ 317. Втручання в роботу телекомунікаційного обладнання (1) Хто перешкоджає або загрожує роботі телекомунікаційного обладнання, що використовується для суспільних цілей шляхом його руйнації, пошкодження, псування, позбавлення електроживлення, карається позбавленням волі на строк до п'яти років або штрафом. (2) Замах карний. (3) Таке діяння, що вчинено з необережності, карається позбавленням волі на строк до одного року або штрафом.	**Стаття 360. Умисне пошкодження ліній зв'язку** Умисне пошкодження кабельної, радіорелейної, повітряної лінії зв'язку, проводового мовлення або споруд чи обладнання, які входять до їх складу, якщо воно спричинило тимчасове припинення зв'язку, - карається штрафом від ста до двохсот неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до одного року, або обмеженням волі на строк до двох років.

Висновки. Керівництво ФРН, розуміючи загрозу національній безпеці через зростаючі масштаби світової кібернетичної злочинності, приділяє велику увагу державній політиці з мінімізації негативних наслідків такої протиправної діяльності. Крім прийняття законодавчих актів, що регламентують вимоги забезпечення захисту інформації в інформаційно-телекомунікаційних мережах Німеччини, Урядом країни затверджена Стратегія кібернетичної безпеки ФРН, яка є головним доктринальним документом із захисту інформаційної інфраструктури країни від кібернетичних атак. Концепція визначає низку дефініцій у галузі кібернетичної безпеки, кібернетичні загрози інформаційній інфраструктурі, об'єкти та суб'єкти посягання, а також організаційні засади протидії протиправним проявам.

Із метою розробки пропозицій із вироблення стратегії державної політики та контроль виконання рішень керівництва держави у сфері протидії кіберзагрозам у ФРН створено вищий дорадчо-консультативний орган – Національну раду кібербезпеки. Для оптимізації оперативного співробітництва між усіма державними установами й поліпшення координації заходів із протидії кібератакам в ФРН створено Національний центр кіберзахисту у сфері управління Федерального відомства захисту інформаційних систем, який безпосередньо взаємодіє із спецслужбами та поліцейськими структурами країни, із приватним сектором Німеччини, країнами-партнерами з ЄС, НАТО, а також міжнародними організаціями.

Така організаційна структура, на думку німецької влади, підвищить рівень захищеності від кіберзагроз не лише національного кіберпростору ФРН, а й більшості країн-партнерів Німеччини за рахунок чіткої та оперативної їх взаємодії.

На думку автора, правові та організаційні засади ФРН із захисту національної інфраструктури від кібернетичних загроз доцільно враховувати під час побудови в Україні аналогічної єдиної національної системи, передусім під час розробки проекту закону України "Про кібернетичну безпеку", який стане базовим у сфері захисту національної інфраструктури від кібератак.

Список використаних джерел

1. Єрменчук О.П. Організація захисту критичної інфраструктури оборонно-промислового комплексу з використанням досвіду США / О.П.Єрменчук, П.П.Скурський // Інформаційна безпека людини, суспільства, держави. – 2011. – № 3. – С. 54-63.
2. Нідільніченко В. Розвиток інформаційних технологій і національна безпека України / В.Нідільніченко // Національна безпека: український вимір. – 2009. – № 3 (22). – С. 43-57.
3. Формирование организационно-правовой системы защиты национальной инфраструктуры от киберугроз / В.В.Бик, А.А.Климчук, В.Н.Панченко, В.В.Петров. – К. : Академпресс, 2013. – 220 с.
4. Матяш О.І. Забезпечення безпеки інформації в Німеччині / О.І.Матяш // Актуальні проблеми управління інформаційною безпекою держави : збір. матер. наук.-практ. конф., Київ, 22 березня 2011 р. – К. : Наук.-вид. відділ НА СБ України, 2011. – Ч. 1. – С. 238-240.
5. Горелихина О.А. Правовая защита персональных данных в Германии / О.А.Горелихина, А.А.Шлиньков // Вопросы экономики и права. – 2012. – № 3. – С. 322-326.
6. Bundesdatenschutzgesetz (BDSG) vom 20.12.1990 [Електронний ресурс] // Офіційний сайт законодавства ФРН. – Режим доступу : http://www.gesetze-im-internet.de.
7. Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG) vom 20.12.1990 [Електронний ресурс] // Офіційний сайт законодавства ФРН. – Режим доступу : http://www.gesetze-im-internet.de.
8. Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes vom 14.08.2009 [Електронний ресурс] // Офіційний сайт Федерального відомства безпеки інформаційних систем ФРН. – Режим доступу : https://www.bsi.bund.de.
9. Cyber-Sicherheitsstrategie für Deutschland vom 23.02.2011 [Електронний ресурс] // Офіційний сайт Федерального відомства безпеки інформаційних систем ФРН. – Режим доступу : https://www.bsi.bund.de.
10. Довгань О.Д. Організаційно-правові засади побудови системи захисту критичної інфраструктури від кібернетичних атак / О.Д.Довгань, І.О.Чернухін // Інформаційна безпека людини, суспільства, держави. – 2012. - № 2(9). – С. 25-33.
11. Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz) vom 01.01.1991 [Електронний ресурс] // Офіційний сайт Федерального відомства безпеки інформаційних систем ФРН. – Режим доступу : https://www.bsi.bund.de.
12. Кримінальний кодекс України від 5 квітня 2001 р. № 2341-III (в редакції від 15 листопада 2011 р.) [Електронний ресурс] // Офіційний сайт Верховної Ради України. – Режим доступу : http://rada.gov.ua.
13. Strafgesetzbuch (StGB) vom 15.05.1871 [Електронний ресурс] // Офіційний сайт законодавства ФРН. – Режим доступу : http://www.gesetze-im-internet.de.

International experience in the field of ensuring information security of person, society, state

Аннотация: В статье проанализированы основные направления государственной политики ФРГ в сфере обеспечения кибернетической безопасности, определены ее ключевые элементы в нормативно-правовых актах Германии: сфера применения, угрозы, объекты и субъекты противоправных проявлений, направления противодействия. Проведен сравнительный анализ уголовного законодательства ФРГ и Украины в сфере обеспечения информационной безопасности.

Ключевые слова: киберугроза, критическая инфраструктура, информационная инфраструктура, киберпреступность, Федеративная Республика Германия.

Abstract: The article analyzes the main directions of the state policy of the Federal Republic of Germany in the field of cyber security, key elements of which are defined in legal acts in Germany: the scope, the threats, objects and subjects of illegal actions, directions of counteraction. A comparative analysis of criminal legislation of Germany and Ukraine in the sphere of information Security.

Key words: cyberthreat, critical infrastructure, information infrastructure, cybercrime, Federal Republic of Germany.