Юридичні науки

УДК 34.096+321.01

Малашко Олександр Євгенійович
викладач кафедри адміністративного права та процесу,
фінансового і інформаційного права
Львівський університет бізнесу та права
Малашко Александр Евгеньевич
преподаватель кафедры административного права и процесса,
финансового и информационного права
Львовский университет бизнеса и права
Malashko Oleksandr
Lecturer of the Department of Administrative Law and Process,
Financial and Information Law
Lviv University of Business and Law
ORCID: 0000-0001-8676-5837

Єсімов Сергій Сергійович
кандидат юридичних наук, доцент,
доцент кафедри адміністративно-правових дисциплін
Львівський державний університет внутрішніх справ
Есимов Сергей Сергеевич
кандидат юридических наук, доцент,
доцент кафедры административно-правовых дисциплин
Львовский государственный университет внутренних дел
Yesimov Serhii
PhD in Law, Associate Professor,
Associate Professor of the Department of Administrative and Legal Disciplines
Lviv State University of Internal Affairs
ORCID: 0000-0002-9327-0071

ЗМІСТ ДЕРЖАВНОЇ ДІЯЛЬНОСТІ ІЗ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
СОДЕРЖАНИЕ ГОСУДАРСТВЕННОЙ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
CONTENT OF STATE ACTIVITIES TO ENSURE INFORMATION SECURITY

Анотація. *У статті в теоретико-прикладному аспекті розглядається зміст державної діяльності із забезпечення інформаційної безпеки. Здійснено аналіз нормативно-правової бази системи забезпечення інформаційної безпеки України, структури органів державної влади, які приймають участь у зазначеній діяльності у контексті державної інформаційної політики. На підставі Доктрини інформаційної безпеки України розглянуто основні аспекти діяльності Верховної Ради України, Президента України, Кабінету Міністрів України, Міністерства цифрової трансформації України, Служби безпеки України, Державної спеціальної служби спеціального зв'язку та захисту інформації України і інших центральних органів виконавчої влади щодо розробки і удосконалення нормативно-правової бази та практичної реалізації заходів, направлених на забезпечення інформаційної безпеки. Зазначено, що для забезпечення ефективного функціонування системи забезпечення інформаційної безпеки України необхідно підвищити ефективність роботи структурних підрозділів із захисту інформації в органах державної влади, організаціях і підприємствах, що призведе до оптимізації роботи відомчих систем забезпечення інформаційної безпеки та підвищенню ефективності функціонування системи забезпечення інформаційної безпеки України.*

Ключові слова: *доктрина, інформаційна безпека, органи державної влади, забезпечення інформаційної безпеки.*

Аннотация. *В статье в теоретико-прикладном аспекте рассматривается содержание государственной деятельности по обеспечению информационной безопасности. Осуществлен анализ нормативно-правовой базы системы обеспечения информационной безопасности Украины, структуры органов государственной власти, участвующих в указанной деятельности в контексте государственной информационной политики. На основании Доктрины информационной безопасности Украины рассмотрены основные аспекты деятельности Верховной Рады Украины, Президента Украины, Кабинета Министров Украины, Министерства цифровой трансформации Украины, Службы безопасности Украины, Государственной специальной службы специальной связи и защиты информации Украины и других центральных органов исполнительной власти по разработке и совершенствование нормативно-правовой базы и практической реализации мер, направленных на обеспечение информационной безопасности. Отмечено, что для обеспечения эффективного функционирования системы обеспечения информационной безопасности Украины необходимо повысить эффективность работы структурных подразделений по защите информации в органах государственной власти, организациях и предприятиях, что приведет к оптимизации работы ведомственных систем обеспечения информационной безопасности и повышению эффективности функционирования системы обеспечения информационной безопасности Украины.*

Ключевые слова: *доктрина, информационная безопасность, органы государственной власти, обеспечения информационной безопасности.*

Summary. *In the article, in the theoretical and applied aspect, the content of state activities to ensure information security is considered. The analysis of the regulatory and legal framework of the information security system of*

Ukraine, the structure of public authorities involved in this activity in the context of the state information policy is carried out. On the basis of the Doctrine of Information Security of Ukraine, considered the main aspects of the activities of the Verkhovna Rada of Ukraine, the President of Ukraine, the Cabinet of Ministers of Ukraine, the Ministry of Digital Transformation of Ukraine, the Security Service of Ukraine, the State Special Service for Special Communications and Information Protection of Ukraine and other central executive bodies for the development and improvement of regulatory-legal base and practical implementation of measures aimed at ensuring information security. It is noted that in order to ensure the effective functioning of the information security system of Ukraine, it is necessary to increase the efficiency of the work of structural units for the protection of information in public authorities, organizations and enterprises, which will lead to the optimization of the work of departmental information security systems and increase the efficiency of the functioning of the information security system of Ukraine.

Key words: *doctrine, information security, public authorities, information security.*

Постановка проблеми. В результаті глобального соціально-економічного розвитку світу роль інформаційної безпеки неухильно зростає, тому можна говорити, що забезпечення інформаційної безпеки стало одним з важливих компонентів забезпечення національної безпеки. Між інформаційною безпекою та державними органами України існує безпосередній зв'язок. При цьому необхідно розглядати органи, що здійснюють державну владу, в якості основної сили, що забезпечує інформаційну безпеку держави із застосуванням засобів організаційно-технологічного та правового характеру. В умовах, коли спостерігається постійне зростання загроз, пов'язаних з можливістю застосування технологій, пов'язаних з інформацією та комунікаціями, для досягнення

кримінальних, терористичних, військово-політичних цілей (у тому числі в такій формі, як інформаційна зброя), необхідно забезпечувати інформаційну безпеку держави та органів, що здійснюють державне управління.

Аналіз останніх досліджень і публікацій. Важливе значення для розробки проблеми мали праці вчених-правознавців В. Б. Авер'янова, О. Ф. Андрійко, В. М. Бевзенка, А. І. Берлача, Ю. П. Битяка, І. Л. Бородіна, Л. К. Воронової, П. В. Діхтієвського, І. С. Гриценка, Є. В. Додіна, Р. А. Калюжного, О. В. Карасса, Л. Є. Кисіль, А. А. Козловського, М. І. Козюбри, Т. О. Коломоєць, В. К. Колпакова, О. В. Кузьменко, В. І. Курила, Є. В. Курінного, В. В. Луця, Р. С. Мельника, В. Я. Настюка, О. І. Остапенка, А. О. Селіванова, Р. М. Скриньковського, Н. П. Тиндик, М. М. Тищенка, О. І. Харитонової, В. В. Цвєткова, Я. М. Шевченко, Ю. С. Шемчушенка та інших.

Мета статті. Метою статті є дослідження змісту державної діяльності із забезпечення інформаційної безпеки.

Виклад основного матеріалу дослідження. Інформаційне забезпечення органів державної влади України є основною умовою для сталого розвитку та ефективного функціонування державних механізмів, проведення процесу державного управління, яке відповідає сучасним міжнародним реаліям, внутрішньодержавним потребам. Реалізація зазначеного забезпечується проведенням єдиних організаційно-технічних заходів на території України органами влади центрального та регіонального рівнів, організаціями та підприємствами щодо забезпечення інформаційної безпеки від внутрішніх і зовнішніх загроз.

Забезпечення інформаційної безпеки визначає наступні компоненти державної політики:

– нормативно-правовий компонент, розробка законодавства в інформаційній сфері, формування принципів проведення державної

політики у сфері захисту інформації, інформаційних ресурсів, інформаційної інфраструктури;

– організаційно-технологічний компонент має на увазі функціонування інформаційно-комунікаційної інфраструктури;

– техніко-економічний компонент передбачає розробку та виробництво інформаційно-комунікаційних технологій;

– соціальний компонент – підготовка фахівців, ефективне використання технічних засобів та інформаційних систем.

Державна політика у сфері забезпечення інформаційної безпеки України проводиться і здійснюється у вигляді прийняття управлінських рішень, які ґрунтуються на законодавстві України, є основним обов'язком органів державної влади та уповноважених посадових осіб. Для здійснення та проведення державної політики, яка повинна бути спрямована на реалізацію національних інтересів України в інформаційній сфері, державною владою формуються:

– концептуальні документи, які визначають перспективи розвитку інформаційної сфери в Україні, в сфері забезпечення інформаційної безпеки – розробляються та приймаються відповідно до положень, закріпленими в Конституції України;

– законодавство в інформаційній сфері, що визначає правила та обмеження в галузі регулювання суспільних відносин в інформаційній сфері;

– організаційне та технологічне забезпечення діяльності держави в інформаційній сфері, організація державного нагляду та контролю, як об'єкта державного управління.

Забезпечення інформаційної безпеки здійснюється регламентуючими документами та нормативно-правовими актами, що визначають вимоги та критерії, загальну організацію робіт із забезпечення інформаційної безпеки, з виробництва та експлуатації систем захисту інформації; порядок

виробництва, зберігання, продажі, передачі, розповсюдження та споживання інформації в різних галузях діяльності (наприклад, політичної, економічної, військової, ліцензійної).

Окремого розгляду потребує нормативно-методичне забезпечення інформаційної безпеки в ключових системах інформаційної інфраструктури, яка включає деякі державні стандарти, які визначають основні терміни та визначення, систему документів і загальні положення, положення про реєстр ключових системах інформаційної інфраструктури, базову модель загроз безпеки інформації в ключових системах інформаційної інфраструктури, загальні вимоги рекомендації.

На даний момент нормативно-правова база в галузі забезпечення інформаційної безпеки в системах критичної інформаційної інфраструктури вимагає прийняття організаційних і нормативно-методичних документів:

– організаційно-розпорядчі документи (положення, інструкції), які регламентують діяльність і визначають засади взаємодії державних органів, господарюючих суб'єктів при вирішенні питань забезпечення інформаційної безпеки на об'єктах критичної інформаційної інфраструктури; комплекс нормативно-методичних документів, які визначають методичні основи організації робіт щодо забезпечення інформаційної безпеки в критичній інформаційній інфраструктурі на державному, відомчому, регіональному та місцевому рівнях; методичні основи аналізу можливих збитків від порушення безпеки інформації в різних класах об'єктів критичної інформаційної інфраструктури та оцінки ефективності забезпечення інформаційної безпеки в критичній інформаційній інфраструктурі; методичні основи організації проведення контрольних заходів щодо перевірки реальної захищеності інформації в критичній інформаційні інфраструктурі.

В умовах швидко мінливого світу з'явилася велика кількість нових

понять (інформаційний тероризм – кібертероризм, кібербезпека, дестабілізація державної управлінської інфраструктури, комп'ютерні атаки, атаки на віртуальні системи, психологічні операції, різні типи інформаційних воєн (кібервійна, мережева війна та ін.), нові високотехнологічні загрози (застосування інформаційної зброї, розробка високотехнологічних засобів розвідки та ін.) цим обумовлюється необхідність постійного розвитку, вдосконалення та оновлення нормативно-правової бази в інформаційній сфері, забезпечення інформаційної безпеки, у галузі регулювання та контролю кіберпростору.

Організаційно-технологічний компонент має на увазі функціонування інформаційно-комунікаційної інфраструктури.

Інформаційна діяльність держави визначається діяльністю органів державної влади, з одного боку, у межах розвитку інформаційної інфраструктури, створення умов для ефективного функціонування, для вільного доступу громадян до інформаційних ресурсів, а з іншого боку, створення законних бар'єрів для доступу громадян до певному виду інформації, розкриття якої завдають значної шкоди особі, суспільству та державі.

У тексті Доктрини інформаційної безпеки України відзначається важливість забезпечення інформаційної безпеки критичної інформаційної інфраструктури [1].

Державна інформаційна політика України реалізується за допомогою формування державними органами влади необхідних правових, економічних, організаційних та інших умов, що сприяють охороні та захисту інформаційної інфраструктури, а особливо критичної інформаційної інфраструктури [2].

Під критичною інформаційною інфраструктурою розуміються об'єкти припинення роботи яких призведе до значних наслідків і втрат для функціонування держави, наприклад, втрата управління державою і

економікою, незворотні зміни в державному управлінні, загрози національній безпеці.

При оцінюванні критичності об'єкта інфраструктури, зазначає О. В. Мельничук, використовуються два загальні аспекти критичності: усередині системи; для суспільства. Критичність усередині системи описується можливостями внутрішньої інфраструктури, зокрема реакцією, спричиненою невдачею складників об'єкта інфраструктури, а також пом'якшенням наслідків. Критичність для суспільства можна виразити через кількість людей, що обслуговують об'єкт інфраструктури на регіональному рівні, та критичний час, швидкість настання невдачі, що вплине на життя або здоров'я громадян [3, с. 23].

У даний час в Україні тільки почалася розробка нормативно-методичних документів, що регламентують забезпечення безпеки критичної інформаційної інфраструктури, в тому числі в галузі забезпечення інформаційної безпеки критичної інформаційної інфраструктури, що передбачено статтею 6 Закону України «Про основні засади забезпечення кібербезпеки України» [4].

Незважаючи на те, що критична інформаційна інфраструктура не часто піддається атакам, варто відзначити, що порушення функціонування критичної інформаційної інфраструктури може спричинити серйозні наслідки, наприклад, видалення файлів з системи, яка відповідальна за моніторинг і подачу води чи електрики на гідротехнічній споруді, або збій в роботі комп'ютерної мережі управління в аеропорту.

Техніко-економічний компонент має на увазі розробку та виробництво інформаційно-комунікаційних технологій. Доктрина інформаційної безпеки України визначила пріоритетним напрямом для державної політики забезпечення інформаційної безпеки України підвищення конкурентоспроможності вітчизняних виробників і компаній, що спеціалізуються на галузі інформаційних технологій, які здійснюють

виробництво та експлуатацію засобів захисту інформації.

З огляду на уповільнених процесів інформатизації в Україні і застарілого вітчизняного програмного забезпечення, засобів інформатизації, засобів захисту безпеки органи влади, організації та підприємства при розробці і функціонуванні систем захисту інформації використовують обладнання і програмне забезпечення іноземного виробництва, не завжди при цьому організовуючи для таких технічних засобів спеціальні перевірки і атестацію технічних засобів обробки інформації, автоматизованих робочих місць, що збільшує ризики несанкціонованого доступу до оброблюваної інформації.

Стратегія національної безпеки України передбачає завершить створення національної системи кібербезпеки, сформує сучасні спроможності суб'єктів забезпечення кібербезпеки і кібероборони та зміцнить систему їх координації [5].

Соціальний компонент має на увазі підготовку фахівців у галузі забезпечення інформаційної безпеки, забезпечення раціонального і ефективного використання технічних засобів та інформаційних систем, що є важливим елементом реалізації державної політики.

Проблема недостатності кадрового забезпечення у галузі інформаційної безпеки, яка за 20 років не тільки не була вирішена, але й загострилася, є одним з головних недоліків в системі забезпечення інформаційної безпеки будь-якої організації і основною причиною успішності атак, проведених з використанням методів соціальної інженерії.

Доктрина інформаційної безпеки України відображає низький рівень підготовки і перепідготовки кадрів, які здійснюють забезпечення у галузі захисту інформації. Зростання координування та масштабності інформаційних атак на критично важливі об'єкти інформаційно-комунікаційної інфраструктури України вимагає забезпечення високого рівня готовності сил і засобів попередження та виявлення комп'ютерних

атак і ліквідації наслідків.

При недотриманні правил обробки та використання інформації, відсутність контролю, регламентів з технічного захисту інформації, розкриття інформації, що циркулює в органах державної влади може знизити ефективність проведеної державної політики. Порушення правил експлуатації технічних засобів, зокрема, відбувається через слабкий контроль керівництва та низького рівня відповідальності за порушення у сфері захисту інформації. Водночас це завдання вирішується у межах функціонуючої системи підготовки, перепідготовки та підвищення кваліфікації кадрів у зазначеній сфері.

Разом з тим наростання нових викликів і загроз в інформаційному просторі обумовлює необхідність прийняття додаткових заходів щодо вдосконалення даної системи. У даний час підготовку фахівців за акредитованими освітніми програмами бакалавр та магістр за спеціальністю «Інформаційна безпека» здійснюють у 59 вищих навчальних закладів України.

Для вирішення даних проблем повинна бути забезпечена адресна підтримка та цільова підготовка фахівців з інформаційної безпеки у межах окремої групи спеціальностей і напрямів підготовки, підвищена ефективність функціонування профільних освітніх організацій, в тому числі за рахунок розвитку матеріально-технічної бази.

Комплексність і взаємопов'язаність завдань щодо вдосконалення кадрового забезпечення безпеки в інформаційній сфері зумовлює необхідність прийняття додаткових заходів нормативно-правового, організаційного та матеріально-технічного характеру. Зокрема, доцільна розробка концепції розвитку кадрового забезпечення у галузі інформаційної безпеки, визначення порядку підвищення кваліфікації, закріплення фахівців у галузі критичної інформаційною інфраструктурою в органах державної влади.

М. Т. Гаврильців зазначає, що загалом політика інформаційної безпеки як суспільне явище має комплексний характер, включаючи внутрішньо та зовнішньополітичні, економічні, технологічні, військові та інші елементи, тому вимагає комплексного підходу. Діяльність органів державної влади повинна спрямовуватися на виконання конкретних завдань у цій сфері й об'єднуватися єдиною метою – надання належних умов для реалізації забезпечення інформаційної безпеки України [6, с. 203].

Доктрина інформаційної безпеки України передбачає, що державна політика, націлена на те, щоб забезпечити інформаційну безпеку в Україні, за допомогою відповідної системи – системи забезпечення інформаційної безпеки України, яка включає:

– діяльність виконавчих органів державної влади, підвідомчих підприємств і установ;

– сукупність методів забезпечення інформаційної безпеки;

– сукупність засобів захисту інформації. Система забезпечення інформаційної безпеки керується, в першу чергу, принципом поділу гілок влади та розмежування предметів ведення на рівнях влади (центральний, регіональний, місцевий);

– система забезпечення інформаційної безпеки в якості пріоритетних напрямів діяльності проводить актуалізацію і оновлення нормативно-правових, керівних і методичних документів щодо захисту інформації в Україні;

– формування середовища для реалізації громадянами конституційних прав на використання та здійснення діяльності в інформаційному просторі;

– координацію роботи органів державної влади України (центральні, регіональні, місцеві), які здійснюють повноваження з забезпечення безпеки інформації;

– здійснення контрольно-наглядових заходів за оцінкою діяльності та станом забезпечення інформаційної безпеки в органах державної влади, підприємствах і організаціях України;

– підготовку висновків на підставі перевірочних заходів щодо загального стану інформаційної безпеки в центральних і регіональних органах державної влади, організацій та установ;

– систематичну діяльність з виявлення загроз в інформаційній сфері і їх джерел, структуризації цілей і завдань забезпечення інформаційної безпеки у галузі оборони, їх реалізації;

– вироблення та визначення пріоритетних напрямів, які передбачають запобігання, адекватне реагування, ліквідацію і усунення наслідків загроз;

– розробку відомчих і регіональних державних програм, спрямованих на підвищення рівня забезпечення інформаційної безпеки, розробку планів заходів, дорожніх карт реалізації відповідних державних цільових програм;

– організацію системи щодо захисту інформації в критичній інформаційній інфраструктурі;

– розробку вітчизняних засобів інформатизації, телекомунікації і зв'язку, засобів захисту інформаційних ресурсів на підставі стандартів Організації Північноатлантичного договору та Європейського Союзу;

– представлення інтересів України в міжнародних організаціях, організація співробітництва та взаємодії з іноземними партнерами в інформаційній сфері.

Доктрина інформаційної безпеки України визначає організаційну основу системи забезпечення інформаційної безпеки, що складається з органів управління та забезпечення інформаційної безпеки, основні функції цієї системи. Але чітко не прописана структура системи забезпечення інформаційної безпеки.

Згідно з Доктриною інформаційної безпеки Президентом України визначається склад системи забезпечення інформаційної безпеки. Систем забезпечення інформаційної безпеки це взаємопов'язана діяльність виконавчих органів державної влади, включених в процес забезпечення інформаційної безпеки країни, в тому числі: центральних органів виконавчої влади (Верховна Рада України, Кабінет Міністрів України, Рада національної безпеки і оборони України та інші); органи місцевого самоврядування; органи судової влади та інші. Забезпечення інформаційної безпеки учасниками процесу здійснюється відповідно до чинного законодавства України.

Керівництво системою забезпечення інформаційної безпеки здійснюється Президентом та Кабінетом Міністрів України, відповідно до повноважень, затверджених Конституцією України здійснюють формування, реорганізацію та скасування державних органів і сил, що забезпечують безпеку інформації в країні; визначають пріоритети для реалізації державної політики в галузі інформаційної безпеки України; визначають механізми реалізації Доктрини інформаційної безпеки та діяльність виконавчих органів державної влади.

В частині забезпечення інформаційної безпеки Верховна Рада України здійснює функції розробки, оновлення, вдосконалення нормативно-правової бази. Кабінетом Міністрів України забезпечується координація роботи центральних органів державної влади та виконавчих органів державної влади щодо забезпечення безпеки інформації. Кабінет Міністрів України здійснює фінансування державних програм у галузі забезпечення інформаційної безпеки.

Рада національної безпеки і оборони України здійснює прогнозування та оцінку загроз інформаційній безпеці України і їх джерел, розробляє пропозиції та рекомендації:

– щодо реалізації механізмів, які здійснюють проведення

державної політики України в інформаційній сфері;

– з координації та вдосконалення діяльності центральних органів державної влади та виконавчих органів державної влади у галузі реалізації державних цільових програм;

– щодо підвищення рівня захисту критично важливих об'єктів інформаційної інфраструктури;

– з розробки проектів нормативно-правових актів.

Центральні органи державної влади в межах, наявної компетенції, виконують обов'язки щодо забезпечення реалізації положень, які містяться в нормах чинного законодавства, положеннях, які визначаються в указах Президента, постановах Кабінету Міністрів України. Центральні органи державної влади розробляють нормативно-правові акти, що регламентують забезпечення безпеки інформації з поданням на розгляд Кабінету Міністрів України.

Виконавчі органи державної влади центрального рівня взаємодіють з виконавчими органами державної влади регіонального рівня на підставі системи взаємодії органів виконавчої влади [7].

Місцеві органи виконавчих державної влади реалізують державну політику в інформаційній сфері, забезпечують практичну реалізацію заходів, спрямованих на захист інформації, взаємодіють з органами місцевого самоврядування в частині роботи з населенням, установами та громадськими організаціями, вносять на розгляд до центральних органів державної влади пропозиції в частині, що стосується розвитку системи забезпечення інформаційної безпеки України. Органи місцевого самоврядування реалізують державну політику в інформаційній сфері на власній території.

Судова влада здійснює заходи пов'язані з фактами порушення інформаційної безпеки, які спричинили наслідки.

Серед основних суб'єктів забезпечення інформаційної безпеки

України, які включені у функціонування системи забезпечення інформаційної безпеки України можна виділити служби забезпечення інформаційної безпеки державних органів, які здійснюють перевірочні та контрольно-наглядові заходи.

Створення, розвиток і забезпечення ефективного функціонування системи захисту інформації в конкретному виконавчому органі державної влади здійснюють служби контролю і нагляду органу виконавчої влади. Як правило, служби, які здійснюють забезпечення функціонування системи захисту інформації, входять до складу апарату виконавчих органів державної влади.

Розглянемо функції та завдання основних виконавчих органів державної влади (територіальні управління, структурні підрозділи та служби), в компетенцію яких входить забезпечення інформаційної безпеки України.

Міністерство цифрової трансформації України є провідним органом державної влади, який здійснює організаційно-правове забезпечення інформаційної безпеки. Відповідно до положення Міністерство здійснює формуванні державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах і на об'єктах інформаційної діяльності, у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку [8].

До органів забезпечення інформаційної безпеки відноситься Служба

безпеки України, до компетенції якої входить забезпечення безпеки України, зокрема, одним з напрямів її діяльності є забезпечення інформаційної безпеки та захист інформації. Згідно з законом «Про Службу безпеки України», дана структура реалізує функції, пов'язані з участю в забезпеченні інформаційної безпеки України. Служба безпеки України здійснює заходи щодо захисту відомостей, що становлять державну таємницю [9].

У компетенцію входить контроль за тим, як дотримується режим секретності в процесі поводження з інформацією, здійснює координацію діяльності виконавчих органів державної влади щодо захисту державної таємниці, має повноваження щодо розробки рішень, які є обов'язковими для виконання У повноваження входять питання формування переліку посадових осіб виконавчих органів державної влади, наділених повноваженнями віднесення тих чи інших відомостей до державної таємниці; формує перелік відомостей, віднесених до державної таємниці, перелік об'єктів України з особливим режимом; здійснює розсекречення та продовження строків засекречування документів; займається організацією заходів з підвищенню кваліфікації фахівців у сфері захисту державної таємниці, в тому числі здійснює підготовку та перепідготовку, що в сучасних умовах є вкрай актуальним, від високопрофесійних кадрів залежить ефективність забезпечення інформаційної безпеки та адекватне реагування на виникаючі інформаційні загрози.

Важливою функцією Служби безпеки, яка більше користується попитом у організацій і підприємств, що використовують в роботі відомості, які становлять державну таємницю, або які хочуть надавати послуги в цій галузі, є видача ліцензій для роботи з секретними відомостями або надання послуг в цій сфері.

Для попередження та ліквідації наслідків комп'ютерних атак на ІТ-ресурси, розташовані на території України, в дипломатичних

представництвах і консульських установах України за кордоном створена та функціонує державна система. Відповідальність за функціонування державної системи забезпечення інформаційної безпеки дипломатичних органів (запобігання кібератак на території України) поклали на Службу безпеки України та Державну службу спеціального зв'язку та захисту інформації України.

Крім безпосереднього забезпечення та контролю функціонування системи забезпечення інформаційної безпеки дипломатичних органів зазначена система здійснює: прогнозування ситуації у сфері інформаційної безпеки, забезпечення співпраці операторів зв'язку і власників інформаційних ресурсів у галузі кібербезпеки, контроль захищеності інформаційних ресурсів і встановлення причин інцидентів інформаційної безпеки.

Служба зовнішньої розвідки України, у контексті забезпечення інформаційної безпеки здійснює функції аналогічні Службі безпеки України на території іноземних держав.

Державна служба спеціального зв'язку та захисту інформації України здійснює свою діяльність в галузі технічного захисту інформації відомостей, віднесених до державної таємниці, проводить єдину державну науково-технічну політику з розробки та використання засобів захисту інформації, організовує роботу системи забезпечення інформаційної безпеки України від технічних розвідок і від витоку інформації технічними каналами [10]. Державна служба спеціального зв'язку та захисту інформації України і її територіальні управління входять до складу органів, що забезпечують національну безпеку України.

Державна служба спеціального зв'язку та захисту інформації України здійснює формування та реалізацію державної науково-технічної політики в сфері боротьби з кібератаками, розробляє методичні рекомендації по їх виявленню, попередженню, по встановленню причин та

ліквідації наслідків.

Державна служба спеціального зв'язку та захисту інформації України займається координацією діяльності органів державної влади, установ і організацій, до компетенції яких входить забезпечення інформаційної безпеки, особлива увага приділяється захисту інформації, яка підлягає обробці технічними засобами; здійснює організаційно-методичне керівництво діяльністю з захисту інформації; надає послуги з сертифікації засобів захисту інформації та ліцензуванню організацій і підприємств в галузі технічного захисту інформації, виробництва засобів захисту та послуги в галузі експортного контролю.

Відповідно до нормативно-правових актів, затверджених Державною службою спеціального зв'язку та захисту інформації України визначаються методи та механізми захисту інформації, засоби, що забезпечують захист інформації, організують технічний захист інформації.

Державне підприємство «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» розробляє стандарти у галузі захисту інформації.

У МВС України для припинення та розслідування правопорушень в інформаційній сфері, для припинення несанкціонованого доступу до комп'ютерної інформації; боротьби зі створенням, розповсюдженням вірусів; боротьби з розповсюдженням контенту в інформаційній мережі Інтернет, забороненим законодавством України створено Департамент кібкрполіції Національної поліції України.

У Державній митній службі України для забезпечення інформаційної безпеки в частині, що стосується протидії іноземним технічним розвідкам та технічного захисту інформації сформовано служба інформаційних технологій.

Серед основних суб'єктів забезпечення інформаційної безпеки України, які включені у функціонування системи забезпечення

інформаційної безпеки України особливе місце займають спеціалізовані підприємства, які здійснюють розробку та виробництво засобів для захисту інформації, надають послуги у галузі забезпечення інформаційної безпеки. Тому від якості розробок засобів захисту інформації та послуг, що надаються в даній сфері, залежить безпека і ефективність функціонування системи інформаційної інфраструктури.

Для того, щоб підприємство могло займатися діяльністю у сфері захисту інформації, виробництвом засобів забезпечення або наданням послуг у галузі захисту інформації, необхідно отримати ліцензію на здійснення конкретного виду діяльності в уповноваженому органі виконавчої влади. Дані підприємства і організації надають такі організаційно-технологічні послуги:

– обстеження та проведення аналізу рівня захисту використовуваних об'єктів інформатизації, вивчення системи документообігу, перевірка організації на відповідність вимогам нормативно-правових документів;

– створення та розвиток системи забезпечення інформаційної безпеки для конкретної організації або підприємства, забезпечуючи захист інформації технічними та організаційно-правовими механізмами;

– організація системи захисту інформації на базі спеціалізованої організації, яка надає послуги із захисту інформації, на договірній основі, (аутсорсинг), таким чином захист інформації забезпечують висококваліфіковані фахівці з профільної організації.

До суб'єктів забезпечення інформаційної безпеки України, які включені у функціонування системи забезпечення інформаційної безпеки України відносяться сертифікаційно-випробувальні центри, лабораторії, атестаційні центри, які здійснюють перевірку та видають сертифікат відповідності засобів інформатизації, перевіряють підприємства на предмет відповідності вимогам для видачі певного виду ліцензії на

здійснення конкретного виду діяльності.

Служби безпеки та захисту інформації підприємств і організацій відносяться до суб'єктів забезпечення інформаційної безпеки України є центральною ланкою системи забезпечення інформаційної безпеки органів державної влади, підприємств і організацій. Обслуговування та використання комплексів забезпечення інформаційної безпеки в органі державної влади, організаціях і підприємствах, згідно зі штатним розкладом здійснюють штатні фахівці у відповідних структурних підрозділах.

Фахівці повинні мати відповідну кваліфікацію та підходити під встановлені вимоги (наявність стажу роботи, відповідного досвіду роботи, освіти, підвищення кваліфікації, перепідготовки, методичні збори).

Керівники структурних підрозділів, які здійснюють забезпечення інформаційної безпеки підприємства або організації, повинні проходити узгодження в Державній службі спеціального зв'язку та захисту інформації України або її територіальному органі. Система забезпечення інформаційної безпеки органів державної влади критична до порушень з боку посадових осіб.

Рішення задач інформаційної безпеки вимагає комплексного підходу забезпечення законності і економічної доцільності, технічної оснащеності та кадрового забезпечення уповноважених служб, координації та взаємодії з компетентними державними органами, тому в України створена та функціонує система забезпечення інформаційної безпеки. Забезпечують діяльність структурних підрозділів із захисту інформації органів державної влади, організацій і підприємств фахівці із захисту інформації.

Недостатній рівень професійної підготовки фахівців з інформаційної безпеки, нерегулярність підвищення ними кваліфікації в сукупності з рядом інших факторів (розвиток нових загроз безпеки інформації) створюють передумови для появи порушень в галузі захисту інформації

(витік інформації, несанкціонований доступ) в органах влади, організаціях і підприємствах, що може привести до прийняття неправильних управлінських рішень і знизити ефективність проведеної державної політики.

Висновки. На основі проведеного аналізу функціонуючої системи забезпечення інформаційної безпеки можна стверджувати, що:

– правові механізми регулювання відносин у сфері забезпечення інформаційної безпеки вимагають уточнення та доопрацювання, в частині розробки більш чітких повноважень органів, які здійснюють контрольно-наглядові заходи і перевірки органів влади, організацій та підприємств щодо дотримання вимог щодо забезпечення захисту інформації. Також доопрацювання і уточнення вимагають технічні регламенти, регламенти атестації державних інформаційних систем, ключових системах інформаційної інфраструктури;

– високі темпи інноваційного розвитку в різних галузях життєдіяльності не дозволяють своєчасно проводити оновлення базових законодавчих документів, які визначають основні цілі, завдання та заходи щодо захисту інформації;

– в Україні політика у сфері забезпечення інформаційної безпеки на рівні держави формується та реалізується центральними та регіональними органами, спеціалізованими організаціями і підприємствами. Законодавством України визначено організаційну основу системи забезпечення інформаційної безпеки, принципи, механізми, напрямки її діяльності;

– не в повній мірі здійснюється ефективне функціонування системи забезпечення інформаційної безпеки України в силу недостатнього рівня професійної підготовки фахівців з інформаційної безпеки структурних підрозділів із захисту інформації органів державної влади, організацій і підприємств;

– для забезпечення ефективного функціонування системи забезпечення інформаційної безпеки України необхідно підвищити ефективність роботи служб безпеки та структурних підрозділів із захисту інформації в органах державної влади, організаціях і підприємствах, що призведе до оптимізації роботи відомчих систем забезпечення інформаційної безпеки та підвищенню ефективності функціонування системи забезпечення інформаційної безпеки України.

Література

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 р. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text
2. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text
3. Мельничук О. Управління критичною інфраструктурою держави: базові методи та критерії ідентифікації об'єктів // Державне управління та місцеве самоврядування. 2019. № 3(42). С. 13–27. URL: http://www.dridu.dp.ua/zbirnik_dums/2019/2019_03(42)/4.pdf
4. Про правові засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII (із змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text
6. Гаврильців М. Т. Інформаційна безпека держави в системі

національної безпеки України // Юридичний науковий електронний журнал. 2020. № 2. С. 200–203. Doi: https://doi.org/10.32782/2524-0374/2020-2/52

7. Система електронної взаємодії органів виконавчої влади (СЕВ ОВВ) (2020). Актуально на 20.05.2020. URL: https://dir.gov.ua/projects/sev-ovv
8. Питання Міністерства цифрової трансформації: Постанова Кабінету Міністрів України від 18.09.2019 р. № 856. URL: https://zakon.rada.gov.ua/laws/show/856-2019-п#Text
9. Про Службу безпеки України: Закон України від 25.03.1992 р. № 2229-XII (із змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text
10. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України: Постанова Кабінету Міністрів України від 03.09.2014 р. № 411. URL: https://zakon.rada.gov.ua/laws/show/411-2014-п#Text