26 серпня 2020 р. № 1057-р. *Урядовий кур'єр* від 01.09.2020. № 168.

2. Кравченко М.В. Система соціального захисту населення як об'єкт державної політики: методологія та практика : моногр. / М.В. Кравченко. К. : 406. Інформ.-аналіт. Агенство, 2012. 451 с.

3. Семяніста С. Судовий захист права на інформацію як складова реалізації соціального права особи. Соціальні права та їх захист адміністративним судом. Збірник матеріалів ІІІ Міжнародної науково-практичної конференції» (м. Київ, 4 вересня 2020 року). Київ: 2020. 424 с. С. 104-108.

4. Про схвалення Стратегії цифрової трансформації соціальної сфери. розпорядженням Кабінету Міністрів України від 28 жовтня 2020 р. № 1353-р. *Урядовий кур'єр* від 31.10.2020. № 212.

5. Арістова І.В., Чернадчук В.Д. Концепція інформаційних правовідносин : сутність та особливості використання у сфері банківської діяльності. *Інформація і право*. 2012. № 3. С. 47-56.

6. Дубич К.В. Механізм державного управління системою надання соціальних послуг: дис. … докт. наук з держ. управл. (25.00.02). Київ, 2015. 437 с.

7. Про затвердження Положення про Єдину інформаційну систему соціальної сфери. Постанова Кабінету Міністрів України від 14 квітня 2021 р. № 404. URL: https://zakon.rada.gov.ua/laws/show/404-2021-%D0%BF#Text

8. Про соціальні послуги: Закон України від 17 січня 2019 року № 2671-VIII. *Відомості Верховної Ради*. 2019. № 18. ст.73

9. Оксьом І.Г. Адміністративно-правові основи регулювання соціальної сфери за умов розвитку інформаційного суспільства. *Публічне право.* № 2. (34)2019. С. 52-60.
УДК 342.9

Блінова Г.О., д.ю.н., доцентка, професорка кафедри цивільного, господарського та екологічного права
Карпенко О.А., студентка другого (магістерського) рівня спеціальності 081 Право
(Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна)

ЕТАПИ СТВОРЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЮРИДИЧНОЇ ОСОБИ

Початок XXI століття ознаменувався новим витком розвитку інформаційних технологій, які стають невід'ємною частиною повсякденного життя, наголошують науковці [1, с. 5]. Технологічний прогрес створює все ширше коло потреб та можливостей для збору та обробки персональних даних, а самі персональні дані знаходять все ширше використання в найрізноманітніших сферах від бізнесу до політики. Їх використання стає багатоаспектнішим і, окрім допомоги в роботі та побуті, вони можуть слугувати для декого інструментом порушення прав та свобод людини, зокрема права на приватність.

Інформаційна безпека є надзвичайно важливим питанням для будь-якої організації чи ділової сфери. Захист даних та персональної інформації є ключовим елементом бізнесу в нашому світі, де кількість інформації збільшується щодня. Отже, етапи розвитку інформаційної безпеки є надзвичайно важливими для розуміння того, як забезпечити безпеку даних та інформації в роботі юридичних осіб.

Основними світовими тенденціями розвитку інформаційної безпеки є: збільшення кількості кібератак та ризиків для безпеки в Інтернеті; застосування різних методів та технологій для забезпечення безпеки в Інтернеті, таких як шифрування даних, аутентифікація користувачів та застосування багаторівневих захистів; розвиток міжнародних стандартів та рекомендацій щодо захисту інформації, наприклад, стандартів серії ISO/IEC 27000 та стандартів NIST; встановлення правових норм та

механізмів захисту інформації на рівні держави, включаючи законодавчі акти та регулятивні вимоги; розвиток професійної галузі з інформаційної безпеки та популяризація знань щодо безпеки в Інтернеті; залучення різних сторін до забезпечення безпеки в Інтернеті, включаючи державні органи, приватний сектор та громадські організації.

Компанії адаптувалися до обмежень пандемії і віддаленої роботи. Водночас загрози інформаційної безпеки стали більш витонченими, а їх кількість збільшилася. Закономірно, що служби безпеки в умовах переходу на віддалену роботу зосередилися на підготовці захищених каналів зв'язку та іншої інфраструктури. Сучасний інформаційний світ вимагає жорстких вимог у підходах до інформаційної безпеки. Кіберзлочинці використовують слабкі місця у віддаленому робочому середовищі та інтерес співробітників до інформації [2].

Розвиток інформаційної безпеки в світі є постійним та динамічним процесом, і вимагає постійного оновлення технологій та методів для захисту інформації

Розглянемо основні етапи розробки концепції інформаційної безпеки юридичної особи: етап 1 - розробка політики інформаційної безпеки; етап 2 – розробка плану дій в разі кризи; етап 3 – захист мережі та даних; етап 4 – тестування та оновлення заходів безпеки; етап 5 – навчання персоналу.

Перший етап включає розробку політики інформаційної безпеки. Це означає встановлення правил та процедур, які дозволяють забезпечити безпеку даних та інформації. Політика повинна враховувати всі можливі загрози, які можуть виникнути, та містити стратегії їх запобігання.

Другий етап включає розробку плану дій в разі кризи. Це означає встановлення процедур в разі надзвичайних ситуацій, наприклад, випадкової втрати даних, вторгнення в систему або кібератаки. План повинен містити стратегії відновлення даних, захисту системи та дій для попередження майбутніх нападів.

Третій етап включає захист мережі та даних. Це означає встановлення необхідних заходів для захисту мережі та даних від потенційних загроз. Це може включати встановлення антивірусного програмного забезпечення, захист від вторгнень, контроль доступу до системи та шифрування даних.

Четвертий етап включає тестування та оновлення заходів безпеки. Це означає регулярне тестування системи на наявність вразливостей та вдосконалення заходів безпеки для виявлення та запобігання потенційних загроз. Також важливо виконувати оновлення програмного забезпечення та системи безпеки, щоб уникнути застарілих методів захисту.

Останній етап включає навчання персоналу. Це означає надання інформації та навичок для працівників, щоб вони могли попереджувати загрози безпеці та вживати заходів безпеки. Це може включати навчання про паролі, захист мережі та даних, впізнавання шахрайства та інші навички

Правові механізми для захисту інформаційної безпеки допомагають забезпечити захист інформації на різних рівнях, від встановлення правил та норм до підтвердження відповідності стандартам та аудиту ефективності заходів захисту інформації. Оскільки інформація є дуже важливим активом для бізнесу та суспільства в цілому, використання правових механізмів може допомогти зменшити ризики порушення інформаційної безпеки та забезпечити захист від потенційних загроз. Такими правовими елементами механізму інформаційної безпеки є : законодавство, стандарти, сертифікація, аудит.

Законодавство установлює правила та норми поведінки стосовно захисту інформації Забезпечує відповідальність за порушення правил і норм.

Стандарти встановлюють вимоги щодо захисту інформації, допомагають створити єдиний підхід до захисту інформації в різних сферах діяльності

Сертифікація підтверджує відповідність системи захисту інформації встановленим стандартам та вимогам, надає довіру стосовно системи захисту інформації.

Аудит оцінює ефективність заходів захисту інформації, виявляє недоліки та рекомендації щодо вдосконалення системи захисту інформації.

Підсумовуючи вищенаведене, можна дійти висновку, що етапи розвитку інформаційної безпеки є надзвичайно важливими для забезпечення безпеки даних та інформації в роботі юридичної особи. Розробка політики безпеки, плану дій в разі кризи, захист мережі та даних, тестування та оновлення заходів безпеки та навчання персоналу – усі ці етапи є ключовими для досягнення максимального рівня безпеки в інформаційному просторі юридичної особи та допомагають створити збалансовану систему інформаційної безпеки.

Список використаних:

1. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. К.: К.І.С., 2015. 220 с. С. 5

2. Захист від кібератак у новому віртуальному світі. URL: https://ko.com.ua/zahist_vid_kiberatak_u_novomu_virtualnomu_sviti_139421

УДК 347.9

Блінова Г.О., д.ю.н., доцентка, професорка кафедри цивільного, господарського та екологічного права
Као Мінь В., студент першого (бакалаврського) рівня спеціальності 081 Право
(Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна)

ПРОЦЕСУАЛЬНІ ПРАВА Й ОБОВ'ЯЗКИ ЕКСПЕРТА: ОКРЕМІ ПИТАННЯ ПРАКТИКИ РЕАЛІЗАЦІЇ У ЦИВІЛЬНОМУ ПРОЦЕСІ

Основними видами експертиз, що призначають суди при вирішенні цивільних справ, є: почеркознавча; авторознавча; технічна експертиза документів; біологічна; екологічна; автотехнічна; стану доріг та дорожніх умов; гірничотехнічна; пожежно-технічна; будівельно-технічна; в галузі охорони праці та безпеки життєдіяльності; електротехнічна; комп'ютерно-технічна; економічна; товарознавча; автотоварознавча; оціночна; експертиза охорони прав інтелектуальної власності; психологічна; мистецтвознавча. Судова експертиза призначається майже у всіх випадках, коли для з'ясування певних обставин справи необхідні спеціальні знання [1].

Судовий експерт, зазначають О. Заяць та О. Скринковський, – це особа, яка володіє спеціальними (професійними) знаннями, необхідними для з'ясування відповідних (конкретних) обставин справи, а також має право на проведення судової експертизи, яка має особливе значення для матеріалів конкретної справи у суді і письмовий висновок щодо якої є самостійним джерелом доказів [2]. Відповідно до п. 2 ст. 74 ЦПК України професійна допомога (юридична, технічна тощо) та консультації спеціаліста не замінюють висновок судового експерта. Крім того, слід взяти до уваги те, що результати своїх досліджень (конкретних питань, обставин, фактів тощо) експерт обов'язково закріплює в експертному висновку (у письмовій формі), який відповідно до ст. 102 ЦПК України має свою чітко визначену процесуальну форму і згідно ст. 76 ЦПК України має силу доказу нарівні з іншими наявними доказами [3].

Судовими експертами можуть бути особи, які мають необхідні знання для надання висновку з досліджуваних питань. Судовими експертами державних спеціалізованих установ можуть бути фахівці, які мають відповідну вищу освіту, освітньо-кваліфікаційний рівень не нижче спеціаліста, пройшли відповідну підготовку та отримали кваліфікацію судового експерта з певної спеціальності. До проведення