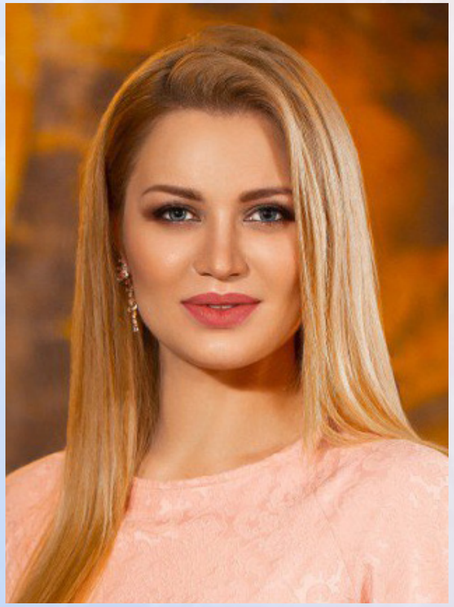
НОТАРІАЛЬНА
ПАЛАТА УКРАЇНИ

Правове регулювання кібербезпеки та захисту персональних даних



ЛЕКТОР

Марина Черниш
Приватний нотаріус київського міського нотаріального округу, член комісії Нотаріальної палати України з питань інформатизації, цифрової трансформації та запобігання кіберзлочинності

Закон України «Про основні засади забезпечення кібербезпеки України»

Кібератака — спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

Кібербезпека — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

Кіберзагроза — наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;

Кіберзахист — сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

Кіберзлочин (комп'ютерний злочин) — суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

Кібероборона — сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;

Кіберпростір — середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

Стаття 4 ЗУ «Про основні засади забезпечення кібербезпеки України»

Об’єктами **кібербезпеки** є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об’єкти критичної інфраструктури.

Об’єктами **кіберзахисту** є:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об’єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки

1) Міністерства та інші центральні органи виконавчої влади;

2) Місцеві державні адміністрації;

3) Органи місцевого самоврядування;

4) Правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) Підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;

8) Суб'єкти господарювання, громадяни України та об'єднання громадян, **інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами,** здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Суб'єкти забезпечення кібербезпеки у межах своєї компетенції:

1) Здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

2) Здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

3) Здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

4) Розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

5) Забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління;

6) Здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.

Серед всіх обов'язків можна виокремити наступні:

- Створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО;
- Встановлення обов'язкових вимог інформаційної безпеки об'єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури;
- Проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;
- Становлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;
- Державно-приватної взаємодії у запобіганні кіберзагрозам об'єктам критичної інфраструктури, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період.

ІНФОРМАЦІЯ — будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

СУБ’ЄКТИ інформаційних відносин відповідно до статті 4 цього ж закону, є

- Фізичні особи;
- Юридичні особи;
- Об’єднання громадян;
- Суб’єкти владних повноважень.

Інформаційна безпека України — складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом.

Додаток 3
до Договору про надання
послуг приватним нотаріусам

ТЕХНІЧНІ ВИМОГИ,
ЩО ПРЕД'ЯВЛЯЮТЬСЯ ДО КОМП'ЮТЕРНОГО РОБОЧОГО МІСЦЯ

м. Київ

1. Апаратне забезпечення:
- окрема персональна електронно-обчислювальна машина (комп'ютер, ноутбук) з підключенням до Інтернет швидкістю не менш 128 кБіт/сек для кожного робочого місця та статичною (фіксованою) IP- адресою*;
- процесор частотою не менше 2 ГГц*;
- оперативна пам'ять не менше 4 Гб*;
- вільний простір на жорсткому диску типу SSD не менше 20 Гб*;
- лазерний принтер формату А4 будь-якої фірми, за умови сертифікації на території України*;
- TWAIN (1.х-2.х) сумісний планшетний сканер формату А4*.

2. Програмне забезпечення:
- ліцензійна операційна система Microsoft Windows 10 або більш новітні версії;
- веб-браузер GoogleChrome, MozillaFirefox, Opera останніх актуальних версій;
- ліцензійне антивірусне програмне забезпечення, що має чинний позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації, зареєстрований в Адміністрації Державної служби спеціального зв'язку та захисту інформації України, з актуальними антивірусними базами даних;
- програмний міжмережевий екран (брандмауер), політика якого унеможливлює віддалений доступ до програмних та апаратних ресурсів комп'ютерного робочого місця, встановлення та роботу додаткових програмних засобів, не пов'язаних із доступом до Систем, та доступ до мережі Інтернет з метою користування електронною поштою та у інших цілях, не пов'язаних із доступом до Систем;
- пакет Microsoft.NET Framework 4.0 та 2.0*;
- програмний комплекс «ІІТ Користувач ЦСК-1»*;
- спеціалізоване програмне забезпечення для роботи з Системами (встановлюється Підприємством).

3. Встановлення/використання Нотаріусом додаткових програмних та технічних засобів (заходів) захисту на комп'ютерному робочому місці, призначеному для роботи з Системами, може бути здійснено виключно за умови наявності позитивного експертного висновку на такі додаткові програмні технічні засоби (заходи) захисту за результатами державної експертизи у сфері технічного захисту інформації, зареєстрованого в Адміністрації Державної служби спеціального зв'язку та захисту інформації України.

4. Встановлення/використання Нотаріусом додаткових програмних засобів (крім випадків, передбачених пунктом 3 цього Додатку 1 до Договору) на комп'ютерному робочому місці, призначеному для роботи з Системами, – ЗАБОРОНЕНО.

5. Здійснення доступу до мережі Інтернет з метою користування електронною поштою та у інших цілях з комп'ютерного робочого місця, призначеного для роботи з Системами, – ЗАБОРОНЕНО.

6. При необхідності використовувати більше одного робочого місця для користування Системами, комп'ютери Нотаріуса мають бути з'єднані у локальну мережу швидкістю не менше 100 мБіт/сек. З'єднання комп'ютерів у локальну мережу Нотаріус забезпечує за власний рахунок.

7. У разі невідповідності комп'ютерного робочого місця цим вимогам, коректна робота програмного забезпечення Систем не гарантується.

ПРИМІТКА:

***** - умови, що в обов'язковому порядку пред'являються до комп'ютерного робочого місця Нотаріуса

Державне підприємство
«Національні інформаційні системи»

04053, м. Київ, вул. Бульварно-Кудрявська, 4
код ЄДРПОУ **39787008**

Нотаріус

Реквізити зазначаються у заяві про приєднання до цього Договору

Деякі питання електронної ідентифікації та електронних довірчих послуг, затверджені постановою Кабінету Міністрів України від 2 лютого 2024 р. № 119. Цією Постановою затверджено:

Положення про формування та виконання Національної програми інформатизації;

Порядок проведення експертизи Національної програми інформатизації та її складових;

Порядок формування та виконання галузевої програми, проекту, робіт з інформатизації;

Порядок формування та виконання регіональної програми, проекту, робіт з інформатизації;

Порядок здійснення моніторингу та проведення оцінки результативності виконання Національної програми інформатизації та її складових.

ІНШІ АКТИ:

Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджені Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 03 липня 2023 року № 570

Положення про систему захищеного доступу державних органів до мережі Інтернет, затверджене Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30 серпня 2023 року № 771.

Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021.

Стратегія інформаційної безпеки, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021.

1.	ДСТУ ISO/IEC 19989-1:2023 (ISO/IEC 19989-1:2020, IDT)	Інформаційна безпека. Критерії та методологія оцінювання безпеки біометричних систем. Частина 1. Структура - Вперше
2.	ДСТУ ISO/IEC 19989-2:2023 (ISO/IEC 19989-2:2020, IDT)	Інформаційна безпека. Критерії та методологія оцінювання безпеки біометричних систем. Частина 2. Ефективність біометричного розпізнавання - Вперше
3.	ДСТУ ISO/IEC 24745:2023 (ISO/IEC 24745:2022, IDT)	Інформаційні технології. Кібербезпека та захист конфіденційності. Захист біометричної інформації - На заміну ДСТУ ISO/IEC 24745:2015 (ISO/IEC 24745:2011, IDT)
4.	ДСТУ ISO/IEC 15408-1:2023 ISO/IEC 15408-1:2022, IDT)	Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель - На заміну ДСТУ ISO/IEC 15408-1:2017 (ISO/IEC 15408-1:2009, IDT)
5.	ДСТУ ISO/IEC 15408-2:2023 (ISO/IEC 15408-2:2022, IDT)	Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 2. Функційні компоненти безпеки - На заміну ДСТУ ISO/IEC 15408-2:2017 (ISO/IEC 15408-2:2008, IDT)
6.	ДСТУ ISO/IEC 15408-3:2023 (ISO/IEC 15408-3:2022, IDT)	Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 3. Компоненти убезпечення. - На заміну ДСТУ ISO/IEC 15408-3:2017 (ISO/IEC 15408-3:2008, IDT)
7.	ДСТУ ISO/IEC 15408-4:2023 (ISO/IEC 15408-4:2022, IDT)	Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 4. Структура для визначення методів оцінювання та діяльності - Вперше
8.	ДСТУ ISO/IEC 15408-5:2023 (ISO/IEC 15408-5:2022, IDT)	Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 5. Попередньо визначені пакети вимог до безпеки - Вперше
9.	ДСТУ ISO/IEC 18045:2023 (ISO/IEC 18045:2022, IDT)	Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Методологія оцінювання безпеки ІТ - Вперше
10.	ДСТУ ISO/IEC 30107-2:2023 (ISO/IEC 30107-2:2017, IDT)	Інформаційні технології. Виявлення атак на біометричне подання. Частина 2. Формати даних - Вперше
11.	ДСТУ ISO/IEC 30107-1:2023 (ISO/IEC 30107-1:2016, IDT)	Інформаційні технології. Виявлення атак на біометричне подання. Частина 1. Структура - Вперше
12.	ДСТУ ISO/IEC 30107-3:2023 (ISO/IEC 30107-3:2017, IDT)	Інформаційні технології. Виявлення атак на біометричне подання. Частина 3. Тестування та звітування - Вперше
13.	ДСТУ ISO/IEC 30107-4:2023 (ISO/IEC 30107-4:2020, IDT)	Інформаційні технології. Виявлення атак на біометричне подання. Частина 4. Профіль для тестування мобільних пристроїв - Вперше
14.	ДСТУ ISO/IEC 29146:2023 (ISO/IEC 29146:2016, IDT)	Інформаційні технології. Методи безпеки. Структура керування доступом - Вперше
15.	ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT)	Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги - На заміну ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT); ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT)/ Поправка № 2:2019 (ISO/IEC 27001:2013/Cor 2:2015, IDT)
16.	ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT)	Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки - На заміну ДСТУ ISO/IEC 27002:2015 (ISO/IEC 27002:2013; Cor 1:2014, IDT); ДСТУ ISO/IEC 27002:2015 (ISO/IEC 27002:2013; Cor 1:2014, IDT)/ Поправка № 2:2019 (ISO/IEC 27002:2013/Cor 2:2015, IDT)
17.	ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT)	Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки - На заміну ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT)
18.	ДСТУ ISO/IEC 27551:2023 (ISO/IEC 27551:2021, IDT)	Інформаційна безпека, кібербезпека та захист конфіденційності. Вимоги до автентифікації непов'язаних об'єктів на основі атрибутів - Вперше


Принципи GDPR
Обмеження зберігання даних
Конфіденційність даних
Законність та прозорість
Точність та актуальність даних
Обмеження цілей обробки даних
Мінімізація обробки даних

Щодо своїх персональних даних клієнти, співробітники, ділові партнери, підрядники, учні, постачальники тощо мають такі права:

- **отримувати інформацію про використання своїх даних;**
- **отримувати доступ до своїх даних:** необхідно надати фізичним особам доступ до даних, що зберігаються (наприклад, надавши доступ до облікового запису або іншим ручним способом);
- **вимагати виправлення своїх даних:** фізичні особи можуть попросити вас виправити неточні дані;
- **вимагати видалення своїх даних;**
- **вимагати обмеження обробки своїх даних:** суб'єкт даних може попросити вас приховати свої дані або обмежити доступ до них. Однак це право застосовується лише в окремих випадках, наприклад, якщо користувача було неналежно проінформовано про цілі збору даних;
- **просити про перенесення своїх даних:** фізична особа може попросити вас передати свої дані до іншої організації;
- **заперечувати:** користувач може заборонити використання своїх даних для різних цілей, наприклад, для адресного маркетингу;
- **вимагати не піддавати свої дані автоматизованій обробці:** у GDPR передбачені суворі правила використання даних для визначення профілів людей та автоматизації рішень на основі цих профілів.

Privacy by Design означає, що захисту персональних даних і приватності має приділятися увага в software development lifecycle (SDLC) ще на етапі планування архітектури, а не наприкінці розробки, як це трапляється зазвичай. Тобто ще під час планування структури застосунку чи сайту треба продумати, як забезпечити захист персональних даних, їх обробку та видалення на вимогу користувачів.

Privacy by default (захист даних з самого початку) — це принцип, який вимагає від компаній розробляти свої продукти та послуги із застосуванням заходів захисту даних з самого початку, за замовчуванням, без будь-яких додаткових дій з боку користувача (суб'єкта персональних даних).

Data Protection Impact Assessment (DPIA) – це процедура оцінки ризиків при обробці персональних даних. Компанія, що здійснює обробку значної кількості персональних даних, в будь якому випадку наражається ризики, пов'язані з викраденням чи неумисної втрати чи розповсюдження персональних даних. Вказана процедура описана GDPR. Ведення DPIA надає змогу не лише виявити ризики, а й демонструватиме високий рівень правової культури компанії у сфері захисту персональних даних.

DPO відповідає за проведення періодичних навчань і доведення до відома працівників компанії, які займаються обробкою персональних даних, вимог GDPR, що безпосередньо стосуються їх роботи. Спеціаліст з захисту персональних даних проводить регулярні перевірки (аудити) дотримання безпеки у сфері своєї компетенції.

Головна мета **data protection officer** – допомагати Вашій компанії у запобіганні витоку персональних даних і порушенні прав суб'єктів персональних даних (фізичних осіб), а також оптимізувати процеси роботи з такими даними всередині підприємства. Крім того, спеціалісти з захисту персональних даних забезпечують контакт між компанією та будь-якими органами контролю, які здійснюють нагляд за діяльністю, пов'язаною зі збором, обробкою і зберіганням персональних даних.