Документаційне обслуговування підприємства

Модуль 2. Контроль за виконанням документів

Тема № 3. Особливості організації роботи з документами.

Тема уроку №29: Сучасні інформаційні технології роботи з документами

Мета: сформувати поняття послуг в сучасному суспільстві, розвивати вміння застосовувати теоретичні знання на практиці, виховувати інтерес до професії.

Матеріал уроку:

Управління документацією є невід'ємною частиною загальної системи управління підприємством, установою, організацією (далі – установою). Інформація належить до основних ресурсів, які використовує установа, поряд з людськими ресурсами, капіталом, матеріалами й технологією. В усіх країнах з високим рівнем розвитку економіки з сер. 1990-х рр. приділяється значна увага методам управління документованою інформацією з огляду на зростання обсягів її автоматизації. Як наслідок, актуальними є дослідження вчених та експерименти практиків у сфері управління документованою інформацією, спрямовані на перегляд технології традиційного діловодства і перехід до створення високоефективних систем управління всім комплексом документаційно-інформаційних ресурсів. Україна не залишилися осторонь цих процесів. У її інформаційній інфраструктурі відбуваються суттєві зміни, зумовлені продовженням інтеграції України до світового інформаційного простору, впровадження прогресивних інформаційних технологій, автоматизації канцелярської праці, що вплинуло на характер документів та діловодства в цілому. Одночасно спостерігається певне відставання вітчизняної теоретичної та методичної бази від потреб сучасної організації роботи зі службовими документами, однією з причин якого виступає відсутність систематичного вивчення зарубіжного досвіду та його творчого застосування у практиці діловодства України [1, с. 3]. Зовнішньою ознакою переходу більшості країн до інформаційного суспільства стало застосування перед назвою держави латинської літери «е», що означає появу «Електронних США» (e-USA), «Електронної Європи» (e-Europe), «Електронної Франції» (e-France), «Електронної Великобританії» (e-Great Britain). Безумовно, в цей ряд входить і Україна, про що свідчить прийняття цільової програми «Електронна Україна» (e-Ukraine). Поняття «Електронна Україна» насамперед включає органи державної влади та місцевого самоврядування, тоді як у західних країнах на першому плані – посилення контролю громадян над урядом, для чого вводяться публічні оціночні показники його діяльності. В Україні таких програм ще немає. Таким чином, метою «електронного уряду» є доступна для всіх оновлювана інформація органів публічної влади. Тільки держава може вирішити завдання створення в режимі он-лайн нових механізмів, які оптимізують спілкування громадян з бюрократичними інстанціями.

Зокрема, надати населенню необхідну для особистого відвідування інформацію щодо розподілу функцій між підрозділами, приймальні години, списку необхідних документів, бланків заяв, анкет. Для вирішення проблеми

переносу в он-лайн формальних відносин з громадянами, а саме для подолання «цифрової нерівності», передбачається відкрити електронні приймальні, але для обслуговування техніки, консультування громадян необхідні фахівці. Таким чином, і в цьому випадку контакт громадян з «електронним урядом» без посередників не стане ефективним, не говорячи про додаткові фінансові витрати та ймовірність черг в електронних приймальнях. Досвід інших країн показує, що там проблема «цифрової нерівності» вирішується за допомогою вже наявної мережі комп'ютерних кафе і клубів. Причому такі клуби на Заході дуже популярні, незважаючи на високий рівень інтернетизації. У США, наприклад, за останні два роки кількість таких клубів зросла в десятки разів. Уряди Великої Британії, Швеції та інших розвинених європейських країн реалізують спеціальні програми з розвитку інтернет-кафе для забезпечення масового доступу населення до мережі Інтернет. В Україні нині діє близько 4 тис. комп'ютерних клубів та Інтернет-кафе, на їхній основі і можна створити систему електронних приймалень. Аналіз проблеми показує, що наша держава ще не готова використовувати переваги, які дає мережа Інтернет, однак за нею перевага у зміцненні своїх позицій в мережі Інтернет, принаймні доти, доки там не з'явилися інші юрисдикції, що не визнають державних кордонів і зможуть скласти їй конкуренцію у віртуальному просторі. Зважаючи на те, що прийняті владою рішення на різних рівнях безпосередньо стосуються життєво важливих інтересів суспільства і покликані забезпечувати стійкий його розвиток, суспільство вкрай зацікавлене в докладному, кваліфікованому і зрозумілому для всіх висвітленні основних питань, пов'язаних з підготовкою і прийняттям рішень. Актуальність цієї проблеми загострилася у зв'язку з розумінням людством, складності й неоднозначності світу, у якому воно живе. А некомпетентність чи безвідповідальність влади занадто часто обумовлює прийняття рішень із непередбачуваними наслідками, після чого порушується стійкість розвитку, виникають конфліктні ситуації. Вихід із такої ситуації вбачається в забезпеченні прав громадян на вільний доступ до інформації та її структуруванні. Дотримуючись цих умов та використовуючи сучасні інформаційні технології, а саме локальних і глобальних комп'ютерних мереж, системи віртуальної реальності, кожен громадянин одержує можливість переконатися в правильності пропонованих заходів, право погоджуватися з ними і вільно висловлювати щодо цього власну думку [2]. Утім, пізній старт розвитку електронних послуг держави в Україні дозволяє уникнути десятирічний досвід помилок, запровадити вже випробувані сучасні моделі, що довели свою ефективність. Міжнародний досвід у цій царині відрізняється досить суттєво. Певною мірою він залежить

не лише від культурних традицій – наприклад, суттєвий ступінь децентралізації влади в Швеції та директивна централізована модель у південній Кореї, – а також від часу, коли ці рішення впроваджувались. Так, країни, які почали впровадження електронних послуг раніше, не могли будувати інформаційні системи із суттєвою концентрацією обчислювальних потужностей. Одже, в таких країнах системи мають ознаки розпорошеності інформаційних ресурсів, що вже сьогодні ставить гостро питання взаємодії або концентрації (Швеція, Норвегія, Німеччина). Ще у 90-ті один з піонерів електронного урядування Фінляндія обрала шлях розмаїття, що, як їм здавалося, відповідало духу децентралізації. Але у 2000-і була змушена витратити 60 мільйонів євро, аби створити єдину платформу для надання уніфікованих електронних сервісів своїм громадянам. Тож, країни, які почали розвиток пізніше, більше схиляються до систем, що задовольняють концепцію one-stop-shop та мають централізовані архітектури (Естонія, Литва, Чехія, Катар та ін.). Централізовані державні портали мають переваги не лише з точки зору зручності для громадян, але й з точки зору реалізації моделі проактивного підходу, рекомендованого ООН – це коли держава матиме змогу спілкуватися з громадянином напряму через його особистий кабінет, запрошуючи на вибори чи надсилаючи повідомлення, що підходить до кінця термін дії ліцензії. У рамках проекту ePUAP єдиний спосіб надання послуг сьогодні реалізує і Польща [3]. Таким чином, для успішної автоматизації управління документованою інформацією в Україні перш за все необхідно: розробити та затвердити стандарти з управління документацією; зобов'язати державні структури полегшити громадянам доступ до їх інформації; розробити концепцію надання населенню послуг он-лайн, основною метою якої було б створення таких умов, коли громадянам надавався однаковий доступ до інформації та послуг всієї адміністративної структури держави, а органи публічної влади були б відкриті цілодобово і без вихідних; подавати пропозиції й одержувати відгуки на них в інтерактивному режимі за допомогою електронної пошти, що дозволить значно спростити процедури масового опитування населення з найрізноманітніших питань; дистанційно надавати послуги нотаріуса, послуги щодо запису актів громадянського стану, реєстрації транспортних засобів, оплати комунальних послуг, надання соціальної допомоги.

Домашнє завдання:

1. § 1, ст.125-129, конспект
2. Яка система документів необхідна для створення керуючої компанії?

Відповіді надсилати на адресу anylesik@gmail.com. В темі листа зазначайте прізвище, групу, назву предмета; в тексті листа – номер та дату уроку.

Модуль 2. Контроль за виконанням документів

Тема № 3. Особливості організації роботи з документами.

Тема уроку №30: Персональні дані та шляхи їх захисту в документа.

Мета: засвоїти поняття персональних даних в сучасному суспільстві, розвивати вміння застосовувати теоретичні знання на практиці, виховувати інтерес до професії.

Матеріал уроку:

Порядок роботи з персональними даними і правила, яким має відповідати Інтернет-магазин:

Порядок збирання, зберігання та обробки персональних даних врегульовано Законом України “Про захист персональних даних” (Закон номер 2297-VI від 1 червня 2010 року).

Позитивним положенням згаданого Закону є можливість врегулювати відносини з користувачем у цифровій формі. Нормами Закону передбачено, що для інформаційно-телекомунікаційних систем, якими серед іншого є веб-сторінки Інтернет-магазинів і їх супутні мобільні додатки, є можливість отримання дозволу в електронному вигляді та врегулювання відносин шляхом укладення “цифрових” публічних договорів приєднання.

Разом з тим, декількох речень на веб-сайті про начебто згоду користувача на обробку його персональних даних буде явно недостатньо. Закон чітко вказує на те, що мета збору і обробки персональних даних має бути сформульована конкретно і доведена до відома користувачів. Крім того, Ви зобов’язані попередити про обсяг відомостей які збираєте, порядок їх обробки і використання, строки зберігання.

Як було сказано, всі наведені питання вирішуються написанням для Інтернет-магазину публічного договору приєднання у формі Політики Конфіденційності або Положення про конфіденційність Інтернет-сайту. Відповідно до Закону згода користувача на обробку персональних даних та вчинення пов’язаних з цим дій має бути однозначною. Тому по кожній позиції відомостей, що Ви збираєте, має бути сформовано оферту та акцепт, з їх закріпленням в тексті публічної угоди.

Відповідальність Інтернет-магазинів за порушення вимог законодавства про персональні дані:

Порушення передбаченого порядку збирання, зберігання, обробки і поширення персональних даних тягне за собою цивільно-правову, адміністративну, а у певних випадках і кримінальну відповідальність. Так, по-перше, користувач може подати на Вас скаргу до Уповноваженого Верховної Ради України з прав людини, а надалі і цивільний позов до суду. По-друге, передбачено адміністративну відповідальність, закріплену у наступних статтях Кодексу України про адміністративні правопорушення:

- стаття 188-39 “Порушення законодавства у сфері захисту персональних даних”;
- стаття 188-40 “Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини”.

Зокрема, частиною 4 статті 188-39 Кодексу передбачено, що недодержання порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб’єкта персональних даних (тобто користувача/покупця), – тягне за собою накладення штрафу на громадян від ста до п’ятисот неоподатковуваних мінімумів доходів громадян, а на підприємців – від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян.

І це все за одне порушення! А скільки користувачів замовляють товар на Вашому сайті щомісяця і залишають при цьому свої персональні дані?

Професійна розробка Положення про конфіденційність або Політики Конфіденційності для Інтернет-магазину в середньому коштує в сотні разів менше за витрати на врегулювання спорів і вирішення інших юридичних негараздів.

Незаконне збирання персональних даних через Інтернет-магазин – підстава для відкриття кримінального провадження.

Якщо збір персональних даних без дозволу користувача призвів до несприятливих для особи наслідків, то Вас можуть притягнути навіть до кримінальної відповідальності за вчинення злочину. Склад злочину передбачено статтею 182 Кримінального кодексу України – “Порушення недоторканності приватного життя”.

Наприклад, за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконну

зміну такої інформації передбачено покарання аж до позбавлення волі. Статтею 182 Кримінального кодексу України передбачено таку санкцію – штраф від п’ятисот до однієї тисячі неоподатковуваних мінімумів доходів громадян або виправні роботами на строк до двох років, або арешт на строк до шести місяців, або обмеженням волі на строк до трьох років.

Той самий злочин, вчинений повторно, або якщо заподіяно істотну шкоду правам, свободам та інтересам особи, тягне за собою ще суворішу відповідальність – арешт на строк від трьох до шести місяців або обмеження волі на строк від трьох до п’яти років, або позбавленням волі на той самий строк.

Домашнє завдання:

1. 1) с.129-134, конспект
2. Пояснити принципи функціонування інтернет-магазину.

Відповіді надсилати на адресу anylesik@gmail.com. В темі листа зазначайте прізвище, групу, назву предмета; в тексті листа – номер та дату уроку.

Модуль 2. Контроль за виконанням документів

Тема № 3. Особливості організації роботи з документами.

Тема уроку №31: Законодавче регулювання персональних даних

Мета уроку: сформувати знання про персональні дані та їх використання, розвивати практичні уявлення про сервіс, виховувати любов до професії.

Матеріал уроку:

Через низький рівень правової обізнаності громадяни часто ігнорують проблеми, пов’язані із захистом власних персональних даних. Пересічна людина як учасник інформаційних відносин, підписуючи різного роду документи, нерідко вимушена ставити себе у нерівні права, у порівнянні з іншою стороною, а подекуди потрапляє у своєрідну рабську залежність якогось «товариства», супермаркета, банка тощо. Продаючи за копійки конфіденційну інформацію, недосвідчена особа навіть не уявляє, ким і задля чого її персональні дані будуть використані.

Активність користувачів соціальних мереж у формуванні баз персональних даних, незліченні факти шахрайства, організована злочинність надзвичайно загострили проблему правового захисту прав фізичних осіб. Нагальною стає проблема створення адекватної нинішнім економічним та соціально-правовим реаліям системи законодавства, що регулює захист персональних даних.

Зокрема, надзвичайна суспільно-політична ситуація, що викликана воєнною агресією Росії, загрожує не лише життю окремих громадян України, але й нації загалом. У зв'язку з цим міжнародно-правові акти дозволяють запроваджувати тимчасові відступи від зобов'язань (дерогацію). Однак такі заходи мають бути врегульовані законодавством згідно з рекомендаціями Ради Європи «Основні напрямки захисту прав фізичних осіб у зв'язку з обробкою персональних даних в інформаційних супермагістралях» від 09.12.1997 р.

Європейське право

Європейську систему законодавства про захист персональних даних складають більше ніж 10 нормативно-правових актів. Серед них варто відзначити такі документи: Регламент Європейського Парламенту і Ради (ЄС) 216/679 від 27.04.2016 р. про захист фізичних осіб при обробці персональних даних, а також про скасування Директиви 95/46/ЄС (Загальний регламент про захист персональних даних) (далі – Регламент 679); Конвенція Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28.01.1981 р. зі змінами 1999 р.; Додатковий протокол до конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 08.11.2001 р.; Директива 95/66/ЄС «Про обробку персональних даних і захист прав осіб у телекомунікаційному просторі» 1997 р. та ін.

Загальноєвропейський досвід захисту прав і свобод людини сформований з урахуванням правозастосовної практики країн Європейського Союзу, судових рішень Європейських співтовариств, міжнародно-правових актів щодо захисту прав і свобод людини. Інститут захисту персональних даних в ЄС ґрунтується на принципах законності, цільової визначеності, мінімальності, об'єктивності інформації, участі суб'єкта персональних даних у здійсненні контролю, обмеження розкриття персональних даних, інформаційної безпеки. Ці принципи мають нормативну силу та є основою для створення нових правових норм у цій сфері правовідносин, вони обов'язкові для уповноважених органів у процесі здійснення правозастосовної діяльності. Законодавство ЄС про захист персональних

даних охоплює весь комплекс правових норм, у тому числі норми-дефініції, уповноважуючі та забороняючі норми.

Відповідно до положень Директив ЄС, персональні дані – це будь-яка інформація, пов'язана з ідентифікованою особою (суб'єктом даних), що зафіксована на будь-якому носії. До цієї категорії потрапляють імена, поштові адреси, конфіденційна інформація, що зафіксована електронними та будь-якими іншими носіями. Введено поняття «контролери даних». Це фізичні особи або організації, які визначають мету і способи обробки персональних даних.

Під обробкою персональних даних Директива ЄС розуміє будь-які операції з персональними даними або їх сукупність, включаючи збір, запис, систематизацію, зберігання, зміну, передачу та розкриття. Основним принципом, на основі якого повинні діяти контролери персональних даних, визнана об'єктивна та неупереджена обробка персональних даних, завдяки якій суб'єкт даних має отримати інформацію про те, хто саме є контролером даних, мету їх обробки та використання, а також надати згоду на використання персональних даних.

Іншими принципами є такі: законність і зрозумілість цілей збору та обробки персональних даних; точна відповідність обсягу запитаних персональних даних цілям їх використання; зберігання персональних даних не більше терміну, обумовленого цілями їх обробки; можливість доступу суб'єкта інформації до своїх персональних даних для їх зміни, уточнення або видалення; створення необхідних технічних та організаційних заходів для забезпечення захисту даних від незаконної або несанкціонованої обробки, випадкової втрати або руйнівного використання.

Регламентом Європейського Парламенту та Ради №45/2001 від 18.12.2000 р. про захист прав приватних осіб засновано новий незалежний інститут Європейського Уповноваженого (омбудсмена) із захисту персональних даних, основним завданням якого є забезпечення поваги права на недоторканність приватного життя, захист персональних даних усіма союзними органами та інститутами, надання консультаційних роз'яснень як за власною ініціативою, так і за зверненнями зацікавлених органів.

Акти ЄС про захист персональних даних вимагають від країн-учасниць ЄС прийняття законодавчих норм, що забезпечують ефективний захист персональних даних від випадкового або незаконного руйнування, втрати, зміни, несанкціонованого розголошення чи доступу (особливо, якщо мова йде про передачу даних за допомогою електронних мереж). Європейський Союз орієнтує країни своїх учасниць на розкриття правового захисту персональних даних через конституційні засади, що містяться в таких

основних правах людини як право на інформаційне самовизначення, право на таємницю листування, поштових відправлень, право на недоторканність житла.

Законодавство більшості європейських держав поділяє персональні дані за критерієм їх «чутливості» на дані загального характеру (прізвище, ім'я, по батькові, дата і місце народження, громадянство, місце проживання) та «чутливі» або вразливі (інформація про стан здоров'я, етнічна належність, ставлення до релігії, ідентифікаційні коди чи номери, відбитки пальців, записи голосу, фотографії, дані про судимість тощо). Для чутливих персональних даних передбачається більш високий ступінь захисту. Зокрема, забороняється збирання, зберігання, використання та передавання без згоди суб'єкта даних саме чутливих, а не всіх без винятку персональних даних. Принагідно зазначимо, що Закон України «Про захист персональних даних» не має такої диференціації.

Стисло відзначимо важливість Регламенту 679, що набрав чинності 25.05.2018 р. і був предметом широкого обговорення в Україні. Це нормативний акт прямої дії, значний за обсягом документ, який детально визначає фактичну сферу його застосування, територіальну дію, основні принципи, пов'язані з обробкою персональних даних, його мету, термін набрання чинності тощо. Регламент 679 є обов'язковим у повному обсязі та підлягає прямому застосуванню у державах-членах ЄС.

Водночас європейські норми щодо захисту персональних даних та процедури їх обробки мають враховуватися в Україні, яка не є членом ЄС. Якщо порівнювати з Директивою 95/46/ЄС, Регламент 679 встановлює більш жорсткі норми, пов'язані з відповідальністю за дотримання законності обробки персональних даних та орієнтує на необхідність запровадження якомога більшого обсягу персональних даних, що підлягають захисту. Держави-члени ЄС мають внести зміни до національного законодавства як для гармонізації норм, так і для прийняття більш детальних правил. Повну оцінку впливу Регламенту 679 на фактичні відносини у сфері обробки персональних даних можна дати лише на основі аналізу практики застосування та наукового аналізу ефективності нового документа.

Національна модель правового захисту персональних даних

Основна роль у формуванні національної моделі механізму правового захисту персональних даних людини й громадянина розкривається через конституційні засади, що містяться у ст. 3, 28, 30, 31, 32, 34, 35, 41, 54, 55, 64 Конституції України та нормативно-правових актах Європейського Союзу. Відсутність у тексті Конституції України спеціально визначеного права на захист персональних даних не є перешкодою для визнання цього права

предметом конституційного захисту, оскільки такий захист передбачений комплексом положень конституційних норм розд. 2 Основного закону.

Національну конструкцію права на забезпечення конфіденційності персональних даних складають Конституція України, Закони України «Про захист персональних даних», «Про інформацію», рішення Конституційного Суду України *(далі – КСУ)*, кодифікаційні акти тощо. Зокрема, відповідно до правової позиції КСУ у справі Устименка К.Г., «...забороняється не лише збирання, але й зберігання, використання та поширення конфіденційної інформації про особу без її попередньої згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту, прав та свобод людини» (Рішення КСУ №5-зп від 30.10.1997 р. у справі щодо офіційного тлумачення ст. 3, 23, 31, 47, 48 Закону України «Про інформацію» та Рішення КСУ від 20.01.2012 р. за конституційним поданням Жашківської районної ради щодо тлумачення ст. 23 Конституції України). Цими ж рішеннями КСУ визначено, що до конфіденційної інформації про особу належать такі свідчення про особу як освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан, інші персональні дані.

Ст. 31 Конституції України гарантує особі захист від втручання в її особисте і сімейне життя, таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. Для іноземців та осіб без громадянства в Україні встановлено національний режим захисту цих прав.

Кодифікаційні акти

Стан захищеності персональних даних багато в чому залежить від здатності чинного законодавства забезпечити збереження у таємниці конфіденційної інформації від тих суб'єктів, які не мають повноважень на ознайомлення з нею і можуть передати таку інформацію третім особам або використати її у протиправних цілях. Цілком логічно, що персональні дані входять до сфери захисту кодифікаційного законодавства за відповідними галузями правового регулювання. Так, ст. 163 Кримінального кодексу України передбачає кримінально-правову відповідальність за порушення таємниці листування, телефонних розмов, телеграфічної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер.

Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та право вимагати вилучення будь-якої інформації, а також право на відшкодовування матеріальної та моральної шкоди, завданої збиранням, зберіганням. використанням і поширенням такої недостовірної інформації. Незаконне збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди або поширення цієї інформації у публічному виступі,

творі, що публічно демонструється, чи в засобах масової інформації є злочином (ст. 182 Кримінального кодексу України).

Цивільним кодексом України *(далі – ЦК)* персональні дані віднесені до особистих немайнових прав і передбачений судовий порядок їх захисту від протиправних посягань. Визнано право власності адресата на надіслані йому листи, телеграми тощо. На публікацію отриманої кореспонденції має бути згода особи, яка її надіслала. Якщо кореспонденція стосується приватного життя іншої фізичної особи, то для її використання (зокрема, шляхом опублікування) потрібна згода цієї особи. Згідно з чинним законодавством, кореспонденція, що стосується фізичної особи, може бути долучена до судової справи лише у тому випадку, якщо в ній містяться докази по суті конкретної справи, а інформація з такого джерела не підлягає розголошенню (ст. 270 ЦК).

Фізична особа має право на таємницю про стан свого здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані під час її медичного обстеження (ст. 286 ЦК). Чинним законодавством заборонено вимагати та подавати за місцем роботи або навчання інформацію про діагноз та методи лікування фізичної особи. Інша особа зобов'язана утримуватися від поширення цієї інформації, якщо така інформація стала відома їй у зв'язку з виконанням службових обов'язків або з інших джерел. Тобто особа, яка має доступ до персональних даних (конфіденційної інформації), зобов'язана не передавати таку інформацію третім особам без згоди її власника. Винятком може бути інформація стосовно вчинених конкретною особою діянь протиправного (кримінально-правового) змісту.

Спеціальні закони

Основним законом, що регулює порядок поводження з персональними даними на території України, є Закон України №2297 від 01.06.2010 р. «Про захист персональних даних» *(далі – Закон)*. Ст. 2 Закону визначає зміст та значення основних термінів, що вживаються в Законі. Зокрема, визначено зміст поняття, що є предметом закону. Персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Недоліком такого визначення є те, що в ньому на концептуальному рівні відсутні критерії, за якими можна відрізнити персональні дані від будь-якої іншої інформації (наприклад, конфіденційної інформації про особу).

Стан гарантованої захищеності персональних даних забезпечується саме на підставі критеріїв-ознак поняття «персональні дані», надійного збереження цих критеріїв-ознак від третіх осіб, які не мають повноважень на ознайомлення з ними. Наразі Закон не охоплює багатоманітність усіх

проблемних правовідносин у сфері захисту персональних даних (Постатейний аналіз Закону за підсумками його обговорення здійснено Головою Державної служби України з питань захисту персональних даних, кандидатом технічних наук Марвинським О.І.).

02.06.2012 р. було ухвалено ще один Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних», яким доповнено зміст ст. 188-39, 188-40, 182 Кодексу України «Про адміністративні правопорушення». Передбачена відповідальність у вигляді штрафу за порушення недоторканності приватного життя. Ефективність зазначених нововведень досить сумнівна, адже персональні дані – це не лише недоторканність приватного життя, але й одна з найбільш мінливих правових категорій, пов'язаних зі стрімким розвитком інформаційних технологій, способів накопичення та обробки інформації стосовно всіх фундаментальних прав людини. Потрібен комплексний підхід до оновлення та вдосконалення положень спеціального законодавства про захист персональних даних, створення дієвих механізмів з нагляду та захисту прав і законних інтересів індивідів відповідно до ст. 28 Директиви 95/46/ЄС.

Право на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції може бути обмежене лише судовим рішенням за наявності підстав, передбачених ст. 6 Закону України «Про оперативно-розшукову діяльність», з метою запобігання злочинам чи з'ясування істини під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо. Ст. 6 Закону України «Про поштовий зв'язок» від 04.10.2001 р. зобов'язує операторів, провайдерів телекомунікацій вживати технічних та організаційних заходів із захисту поштових відправлень, телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом та інформації, що передається цими мережами.

Враховуючи специфіку правових відносин, захист персональних даних передбачається Основами законодавства про охорону здоров'я від 19.11.1992 р. (ст. 40); Законами України «Про нотаріат» (ст. 8), «Про адвокатуру» та ін.

Порівняльний аналіз законодавства України про захист персональних даних дає змогу зазначити, що для повного приведення національного законодавства у відповідність зі стандартами ЄС потрібні додаткові організаційно-правові заходи щодо вдосконалення контролю за виконанням законів і підзаконних актів у цій галузі та доповнення їх змісту за моделями Міжнародної та Європейської Конвенцій про захист персональних даних, ухвалених у новітній час Директив ЄС.

Домашнє завдання:

1. Підручник 1, с. 136-142, написати конспект
2. Проаналізувати законодавчо-правову базу, що регламентує кібербезпеку.

Відповіді надсилати на адресу anylesik@gmail.com. В темі листа зазначайте прізвище, групу, назву предмета; в тексті листа – номер та дату уроку.

Модуль 2. Контроль за виконанням документів

Тема № 3. Особливості організації роботи з документами.

Тема уроку №32: Особливості захисту та зберігання даних сучасних цифрових сервісів

Мета: сформувати поняття документаційного обслуговування в сучасному суспільстві, розвивати вміння застосовувати теоретичні знання на практиці, виховувати інтерес до професії.

Матеріал уроку:

Дані — це найцінніший корпоративний актив для будь-якого бізнесу. Незалежно від того, в якій галузі працює підприємство, важливо дбати про фінансові звіти та медичні записи або бізнес-плани для стартапу. База даних (БД) — це структурована сукупність інформації, яку можна зберігати, аналізувати та обробляти за допомогою СУБД (системи управління базами даних). Бази даних необхідно захищати та регулярно перевіряти актуальність цього захисту. Використовуючи спеціальні програми та методики, можна запобігти несанкціонованому доступу (НСД) до бази даних в локальних мережах або витоку інформації, не призначеної для широкого розголосу.

Жодне підприємство, корпорація, державна установа не може обійтися без використання інформаційної бази (клієнтів, нормативних актів, продуктів, фінансової звітності). Такі масиви майже завжди містять персональну, корпоративну та конфіденційну інформацію. Її викрадення може призводити до катастрофічних наслідків як фінансового, так і репутаційного характеру.

Є дві основні причини, що змушують приватні компанії та державні установи витрачати все більші суми на захист БД.

По-перше, це кіберзлочинність. Постійне вдосконалення інструменту зловмисників, поява нових програм-вимагачів, безфайлові способи проникнення і ризик того, що хтось зі співробітників виконає дії, що несуть загрозу конфіденційної інформації. Тільки за 2019 рік, згідно з дослідженнями Data Breach QuickView Report, було розкрито понад 9 мільярдів облікових записів, що містять персональну інформацію. За розвитком злочинних технологій розвиваються і рішення, що допомагають захистити таємні відомості. Важливо вживати превентивні заходи, такі як налаштування конфігурації брандмауера, для обмеження доступу до вхідного

і вихідного підозрілого трафіку, а також реалізувати рішення і процедури на випадок небажаного порушення безпеки.

По-друге, це проблема відповідності. Міжнародне законодавство щодо захисту персональної інформації постійно вдосконалюється і стає все більш жорстким. Відповідальність за недоторканність конфіденційних відомостей покладається на організації, які їх збирають в процесі своєї діяльності. Причому в залежності від галузі та типу інформаційних активів, нормативні вимоги можуть істотно відрізнятися. Щоб бути конкурентними на ринку, українським компаніям необхідно відповідати цим стандартам, вкладати більше фінансових ресурсів в забезпечення захисту БД.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

Що таке безпека даних? Це важлива частина загальної стратегії захисту. Вона включає методи виявлення та оцінки загроз безпеки і зниження ризиків, пов'язаних із захистом конфіденційної інформації та лежать в основі комп'ютерних систем і мережевої інфраструктури.
У цьому контексті важливо розуміти, що захист даних і безпека БД — це не одне і те ж.

Процес захисту даних інформаційної бази передбачає активні дії щодо забезпечення безпеки. Захист систем баз даних — це сукупність методів, програмних засобів, процесів, програм та технологій, застосування яких забезпечує безпеку інформації, що зберігається і запобігають її від несанкціонованого електронного доступу, модифікацій, випадкового розкриття, порушення, знищення, копіювання.

Безпека БД пов'язана з пасивними заходами, які в основному стосуються політики конфіденційності. Вони визначають, як корпорації обробляють і управляють наявними в їх розпорядженні масивами, особливо конфіденційними, такими як особиста інформація, дані кредитних карт, медичні або освітні записи.

Загальновідоме правило — захист баз даних повинен бути багаторівневим. Це означає, що для того, щоб запобігати несанкціонованому доступу до бази даних або її копіювання, необхідно провести комплекс заходів. Чим більше рівнів захисту, тим більше зусиль і програмних засобів знадобиться

зловмисникові для злому. І починатися багаторівнева система безпеки повинна з контролю на рівні користувача. Захист бази даних на первинному етапі полягає в умінні розподіляти процеси, привілеї та права доступу. Загроза інформації може бути не тільки зовнішньою, але й внутрішньою. Більше можливостей отримати несанкціонований доступ і копіювати дані — у співробітників підприємства. Причому це може бути зроблено, як навмисно, так і випадково.

Тому захист на початковому рівні передбачає ефективне обмеження несанкціонованого доступу. Засоби контролю перевіряють справжність розподілених прав користувачів і додатків, обмежуючи їх доступ до БД: надання відповідних атрибутів та ролей користувачів, а також обмеження адміністративних привілеїв.

Домашнє завдання:

1. 1, ст.125-126, конспект
2. Пропишіть ОСНОВНІ КОНЦЕПЦІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ.

Відповіді надсилати на адресу anylesik@gmail.com. В темі листа зазначайте прізвище, групу, назву предмета; в тексті листа – номер та дату уроку.