

Інформаційна безпека:

анотований бібліографічний список

2020. – Вип. 10 (жовтень). – 6 с.

<http://www.nplu.org/article.php?id=423>

1. **Бондарь М. Ваш профиль не удален** / Мария Бондарь // Фокус. – 2020. – № 30 (9 жовт.). – С. 44-45. *У контексті того, що поліція збирається ставити на облік українських користувачів російської соціальної мережі "Вконтакте", з'ясовано, що загрожує громадянам України, зареєстрованим у цій мережі. Нагадано, що секретар Ради національної безпеки і оборони України (РНБО) Олексій Данілов оголосив про наміри правоохоронців на конференції "Перспективи диджиталізації країни та ризики кібербезпеки". Наведено коментарі юристів, зокрема, представників компанії "Лабораторія цифрової безпеки", "YouControl" та ін. Фахівці зазначають, що в українському законодавстві немає єдиної норми, що передбачає якусь відповідальність за відвідування заборонених сайтів. Акцентовано увагу на ст. 34 Конституції України, що декларує свободу слова, думок і способу висловлення поглядів і переконань, яка може бути обмежена спеціальним законом у цілях національної безпеки. Також зауважено, що у своїй заяві О. Данілов згадав Національну поліцію, яка не має права розглядати справи щодо таких правопорушень. Підсумовано, що органи держбезпеки повинні відслідковувати розпалювання сепаратистських настроїв, причому на будь-яких платформах, а не тільки в мережі "Вконтакте".*

2. **Бурячок В. Л. Безпека безпроводових і мобільних мереж** : навч. посіб. / Володимир Бурячок, Володимир Соколов, Махіяр Тадждіні ; Київ. ун-т ім. Б. Грінченка. – Київ : Київ. ун-т ім. Б. Грінченка, 2020. – 143 с. : іл., табл. **Шифр зберігання в Бібліотеці: А807194** *Розкрито практичні аспекти організації та забезпечення безпеки безпроводових і мобільних мереж. Висвітлено основні способи боротьби з уразливостями, що притаманні таким мережам, та запропоновано шляхи виявлення загроз на проникнення з метою унеможливлення доступу зловмисників до таких мереж. Охарактеризовано*

спеціалізоване мережеве обладнання, що може бути застосоване для проектування з урахуванням загроз систем захисту безпроводових і мобільних мереж. Посібник містить основні відомості про методи захисту інформації в безпроводових і мобільних мережах, методичні вказівки про порядок проведення відповідних лабораторних робіт, вимоги до оформлення висновків.

3. **Бурячок В. Л. Основи інформаційної та кібернетичної безпеки :** навч. посіб. / В. Л. Бурячок, Р. В. Киричок, П. М. Складанний ; Київ. ун-т ім. Б. Грінченка. – Київ : Київ. ун-т ім. Б. Грінченка, 2020. – 434 с. : іл., табл. **Шифр зберігання в Бібліотеці: A807195** Посібник містить теоретичний і практичний матеріал стосовно сучасних проблем інформаційної та кібернетичної безпеки, а також методичні, наукові та практичні рішення для підвищення рівня знань студентів у цій сфері. Також представлено низку лабораторних робіт, згрупованих за трьома розділами: «Кібернетичний простір, мережа Internet та система WWW», «Теорія інформаційної безпеки», «Методологія захисту інформації». Наведені теоретичні відомості сприятимуть більш глибокому та детальному розгляду основних положень, понять і визначень базових аспектів захисту інформації, створення та експлуатації захищених інформаційних та комунікаційних систем.

4. **Доронін І. М. Національна безпека України в інформаційну епоху: правові аспекти :** монографія / І. М. Доронін ; НДІ інформатики і права НАПрН України. – Київ : АртЕк, 2019. – 433 с. **Шифр зберігання в Бібліотеці: A807028** У монографії розглянуто еволюцію концепту «національна безпека» у вітчизняній правовій науці в інформаційну епоху. Досліджено передумови виникнення, а також процеси розвитку і трансформації національної безпеки України, правові засади її забезпечення. Окремо проаналізовано вплив факторів агресії проти нашої держави та еволюції інформаційного суспільства на стан забезпечення національної безпеки і трансформації системи її забезпечення. Крім цього, досліджено складний характер суспільних змін в інформаційну епоху в сучасному світі, які зумовлюють зміни у парадигмі правового регулювання. Запропоновано розглядати «право національної безпеки» як галузь права в умовах зміни традиційних підходів до його систематизації.

5. **Інформаційна безпека: проблеми приватного права** : навч. посіб. / [Є. О. Харитонов та ін. ; голов. ред. Є. О. Харитонов] ; Нац. ун-т "Одес. юрид. акад.", Ф-т цивіл. та госп. юстиції, Каф. цивіл. права. – Одеса : Юрид. літ., 2019. – 274 с. **Шифр зберігання у Бібліотеці: A807239** Викладено основи правового забезпечення інформаційної безпеки, охарактеризовано правопорушення в інформаційній сфері. Розглянуто основні приватноправові способи забезпечення інформаційної безпеки, особливості забезпечення прав інтелектуальної власності в інформаційній сфері, цивільно-правової відповідальності та застосування спеціальних знань (експертизи) у сфері забезпечення інформаційної безпеки.

6. **Кукін І. В. Особливості зворотних зв'язків у системі національної безпеки держави** / І. В. Кукін // Вчені зап. Тавр. нац. ун-ту ім. В. І. Вернадського. Серія : Держ. упр. – Київ, 2019. – Т. 30 (69), № 4. – С. 153-157. *Наведено результати дослідження зворотних зв'язків у соціальних системах та їхній вплив на гарантування інформаційної безпеки особистості та національної безпеки держави. Визначено основні різновиди і функції зворотних зв'язків у сфері національної безпеки й інформаційної безпеки особистості. Зазначено, що зворотні зв'язки суттєво впливають на основні властивості соціальних систем, стан інформаційної безпеки особистості та національної безпеки держави. Залежно від панівної в суспільстві форми культури їх можна розподілити на раціональні (відповідають досягнутому рівню знань у сферах науки та техніки), чуттєві (формуються під впливом емоцій людини), ідеальні (базуються на панівних у суспільстві релігійних канонах), обмежено інтегральні (включають декілька із зазначених різновидів) та інтегральні (включають усі без винятку їхні різновиди зворотних зв'язків). Основними функціями зворотних зв'язків у соціальній системі, що впливають на стан інформаційної безпеки особистості та національну безпеку держави, можуть бути: стабілізація суспільних відносин, накопичення знань про суб'єкт і об'єкт (об'єкти) управління, перетворення в соціальних системах об'єктів на суб'єкти управління, реалізація функцій державного управління, примус щодо дотримання правової поведінки, підтримання іміджу суб'єкта управління,*

забезпечення реалізації основних процесів управлінської діяльності. Текст:
http://www.pubadm.vernadskyjournals.in.ua/journals/2019/4_2019/29.pdf

7. **Науменко Н. Ю. Модифікована модель синтезу системи інформаційної безпеки на регіональному рівні** / Н. Ю. Науменко // Причорномор. екон. студії. – 2019. – Вип. 42. – С. 138-144. *Запропоновано концептуальну модель процесу синтезу та функціонування системи інформаційної безпеки регіональної соціально-економічної системи. Здійснення синтезу системи інформаційної безпеки з теоретичної та практичної точок зору базується на вирішенні зовнішніх та внутрішніх протиріч. Розроблено алгоритм послідовного розв'язання основних задач за технологічною схемою аналізу системи інформаційної безпеки у сфері економічної безпеки регіону. Отримано модель із семи взаємопов'язаних послідовних етапів, реалізація яких забезпечує обґрунтування та вибір оптимального варіанта конфігурації та технології забезпечення економічної безпеки регіону за компонентом інформаційної безпеки регіональної соціально-економічної системи.* Текст:
http://www.bses.in.ua/journals/2019/42_2019/28.pdf

8. **Технології забезпечення безпеки мережевої інфраструктури :** підручник [для аспірантів та магістрантів закл. вищ. освіти, які навчаються за спеціалізацією "Безпека інформаційно-комунікаційних систем" спец. 125 "Кібербезпека" галузі знань 12 "Інформаційні технології" / В. Л. Бурячок та ін.] ; Київ. ун-т ім. Б. Грінченка. – Київ : Київ. ун-т ім. Б. Грінченка, 2020. – 281, [1] с. : іл., табл. **Шифр зберігання в Бібліотеці: A807196** *Висвітлено основні способи боротьби з уразливостями різних телекомунікаційних технологій. Розкрито методи організації захищеної передачі даних у незахищеному середовищі. Докладно розглянуто спеціалізоване мережеве обладнання, що застосовується для проектування корпоративних проводових телекомунікаційних систем та мереж, а також забезпечення (з урахуванням загроз) їх безпеки.*

9. **Торічний В. О. Особливості державного управління регіональними системами інформаційної безпеки** / В. О. Торічний // Вчені зап.

Тавр. нац. ун-ту ім. В. І. Вернадського. Серія : Держ. упр. – 2019. – Т. 30 (69), № 3. – С. 180-182. *Визначено основні напрями діяльності держави щодо забезпечення інформаційної безпеки регіону. Окреслено проблеми побудови регіональних систем інформаційної безпеки. Виокремлено методи державного управління регіональними системами інформаційної безпеки.* Текст: http://www.pubadm.vernadskyjournals.in.ua/journals/2019/3_2019/33.pdf

10. **Ханін С. Захист персональних даних** / Семен Ханін // Юрид. газ. – 2020. – 13 жовт. (№ 19). – С. 22 – 23. *Йдеться про захист персональних даних адвокатів та їх клієнтів. За словами автора статті, насамперед необхідно встановити в офісі сигналізацію, яка буде сповіщати не тільки постачальника послуг, але і клієнтів, надсилаючи фотографію кімнати, в якій спрацював датчик. У всіх кімнатах мають бути встановлені відеокамери відкритого базування, а в дубль їм — обов'язково такі ж камери прихованого базування. Сервер, на який пишеться інформація, має знаходитися за межами офісу, а в ідеалі й за межами України. Для цього в інтернеті пропонується достатня кількість послуг з оренди серверного простору в міжнародних дата-центрах. З огляду на те, що українські правоохоронці можуть під час обшуку підкинути печатку або вкрати гроші, все обладнання має працювати з хорошою роздільною здатністю і підключатися через джерело безперебійного живлення. Фізично документи без крайньої необхідності в офісі зберігатися не повинні. Всі документи необхідно сканувати відразу після отримання і зберігати, на віддаленому іноземному сервері. Для зберігання «живих» документів можна використовувати віддалене сховище, у крайньому випадку, наприклад, велику банківську скриньку в банку недалеко від офісу. Розглянуто інші поради щодо захисту персональних даних.* Текст: <https://yur-gazeta.com/dumka-eksperta/zahist-personalnih-danih.html>

11. **Цифрове врядування** : монографія / [О. В. Карпенко та ін.] ; за ред. Олександра Валентиновича Карпенка; Нац. акад. держ. упр. при Президентові України, [Каф. інформ. політики та цифр. технологій]. – Київ : НАДУ, 2020. – 335 с. **Шифр зберігання в Бібліотеці: БЗ63179** У монографії подано наукове обґрунтування теоретичних засад цифрового врядування та надано практичні

рекомендації щодо його впровадження в Україні. Проаналізовано вплив цифрової економіки на розвиток сучасного суспільства в контексті виробництва, використання та споживання digital-технологій. Досліджено особливості формування стратегії цифровізації Республіки Польща. Обгрунтовано необхідність застосування цифрових комунікацій у діяльності органів публічної влади. Розкрито особливості формування цифрової культури в публічному управлінні. Охарактеризовано сучасний стан та визначено перспективи цифрової безпеки. Акцентовано увагу на цифровій безпеці діяльності органів публічної влади. Проаналізовано кібербезпеку як складову цифрових трансформацій. Запропоновано інструментарій та напрями удосконалення цифрової партисипації в публічному управлінні.

12. **Чадюк М. Комунікація (не) за правилами** [Електронний ресурс] / Марія Чадюк // День. – 2020. – 2 жовт. (№ 186/187). – Електрон. дані. У контексті проведення дискусії Донбас-медіафоруму «Дезінформація у когнітивному просторі українського суспільства: які наративи поширюються та як їх викривати» розглянуто питання стосовно того, якою є головна мета російської пропаганди, як не втратити в пастку правил демократії та що варто зробити, щоб зменшити негативний вплив. Акцентовано увагу на питаннях інформаційної безпеки, які все частіше порушуються в публічних дискусіях. Адже хоч головні наративи російської пропаганди переважно не змінюються, проте іншими стають способи й засоби трансляції цих ідей. Текст: <https://day.kyiv.ua/uk/article/media/komunikaciya-ne-za-pravylamy>

Підготовлено відділом інформаційного забезпечення органів влади

Національної бібліотеки України імені Ярослава Мудрого

Відповідальний за випуск: Зайченко Н. Я.

29.10.2020

