

СПИСОК ЛІТЕРАТУРИ

1. Горбачова І.В. Управління кадровими ризиками в умовах ринку. *Україна: аспекти праці*. Київ, 2014. № 8. С. 37–42.
2. Калініченко Л. Л. Управління кадровим ризиком на основі застосування когнітивного моделювання. *Ефективна економіка*. 2012. № 7. Режим доступу: http://nbuv.gov.ua/UJRN/efek_2012_7_30 (дата звернення: 17.11.2022).

УДК 351.746:007(100)+(477)

НЕЧИПОРЕНКО Юлія

здобувач вищої освіти 3-го курсу освітнього ступеня «бакалавр»

*Миколаївський національний аграрний університет,
м. Миколаїв, Україна*

Науковий керівник: - **КУШНІРУК Віктор.**,
канд. екон. наук., доцент

*Миколаївський національний аграрний університет,
м. Миколаїв, Україна*

ІНФОРМАЦІЙНА БЕЗПЕКА ЗАГАЛОМ ТА В УКРАЇНІ

Сучасне суспільство є основним генератором інформаційного середовища та повноцінним його споживачем. Виходячи з цього факту, можна з упевненістю сказати, що в міру розвитку цього явища, існують внутрішні безперервні зв'язки та залежності між користувачами глобального чи індивідуального інформаційного простору. З того часу коли невеликі групи людей почали формувати племена, поселення, міста, імперії, і закінчуючи сьогодні, з плином часу, серед таких людей, або, якщо говорити про останній період розвитку суспільства, то в людино-машинних інфраструктурах почали з'являтися накопичення інформації, які з тих чи інших причин не розголошувалися або не могли бути розголошені – простіше іншими словами, всередині системи обміну інформацією з'явилися секрети.

До 19 століття все шифрування було «вручну», тобто виконувалося повністю вручну людиною. З появою складних обчислювальних механізмів і обертових машин, частина цього завдання лягла на механізми. Але коли в життя людства було вторгнуто потужні ЕОМ - комп'ютери, роль людини в цьому процесі була зведена до мінімуму і полягала в розробці таких алгоритмів шифрування нового покоління, які дали б здатність таким чином перетворювати інформацію, використовуючи силу комп'ютерну техніку, щоб ворог жодним чином не зміг її розсекретити. Складність методів і алгоритмів шифрування зростає прямо

пропорційно швидкому розвитку самих комп'ютерів. На сьогоднішній день розроблено багато алгоритми шифрування, які достатньо здатні зберігати цілісність і конфіденційність інформації, враховуючи сучасні можливості комп'ютера та комп'ютерної техніки. Найпопулярніші на сьогодні алгоритми інформаційного середовища - симетричні алгоритми - DES, 3DES, AES, - і асиметричні алгоритми, такі як, наприклад, набір шифрів RSA зі змінною довжина ключа.

З метою протидії масштабним негативним інформаційно-психологічним впливам пріоритетними напрямками національної інформаційної політики мають стати: 1) концептуальне переосмислення інформаційних завдань, які стоять перед українською владою та суспільством загалом; 2) захист українського інформаційного простору від пропагандистської аудіовізуальної та друкованої продукції країни-агресора – Російської Федерації; 3) потужна фінансова, інформаційна та інституційна підтримка розвитку українського кінематографу, телевізійного контенту, радіопростору та друкарство; 4) побудова своєї ефективної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства; 5) модернізація системи інформаційної безпеки держави та формування та реалізація ефективної інформаційної політики; 6) удосконалення законодавства у сфері інформаційної безпеки, погодження національного законодавства з міжнародними стандартами та дієве правове регулювання інформаційних процесів; 7) розвиток національної інформаційної інфраструктури; 8) стимулювання підвищення конкурентоспроможності вітчизняної інформаційної продукції та інформаційних послуг; 9) забезпечення потужної інформаційно-комунікативної присутності у міжнародному інформаційному просторі .

Особливо складною сьогодні є проблема передчасного створення коштів, необхідних для інформаційного протистояння, або, якщо користуватися американською термінологією, – «інформаційної війни».

Комісія з питань національної безпеки визначила такі потенційні загрози в інформаційній сфері: відсутність у міжнародної спільноти об'єктивного уявлення про Україну; інформаційна експансія з боку інших країн; відтік інформації, що містить державну таємницю, а також конфіденційної інформації, яка є власністю держави; повільне входження України у світовий інформаційний ринок; незбалансованість державної політики та відсутність необхідної інфраструктури в інформаційній сфері.

Необхідність у комплексному та ефективному підході до процесу забезпечення безпеки національного інформаційного простору постійно зростає. Актуальним на сьогодні залишається визначення чітких завдань та відповідальних суб'єктів за інформаційну безпеку. Визначаючи цілі, принципи, правові складові, доктрина має стати основою розробки проектів, концепцій, стратегій, цільових програм та планів дій щодо забезпечення інформаційної безпеки України; базою для вдосконалення норм та юридичних осіб механізмів системи захисту інформації у державі.

Діяльність органів державної влади має спрямовуватись на виконання конкретних завдань у цій сфері та об'єднуватись єдиною метою – надання належних умов забезпечення інформаційної безпеки України. Узгоджена діяльність із забезпечення інформаційної безпеки на основі єдиних правових норм сприятиме ефективному інформаційному протистоянню погроз; попередження, реагування та розслідування будь-яких посягань на інформаційну безпеку України.

СПИСОК ЛІТЕРАТУРИ:

1. Кузавков В. В., Хусаїнов П. В. Прогнозування технічного стану однотипних програмно-апаратних засобів. Інформатика та математичні методи в моделюванні. 2018. № 1, С. 57-68.
2. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Humanitarian vision. 20167 Vol. 2, № 1.
3. Рудий Т. В., Сенік В. В., Рудий А. Т., Сенік С. В. Організаційно-правові, криміналістичні та технічні аспекти протидії кіберзлочинності в Україні. Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична / гол. ред. Р. І. Благути. Львів : ЛьвДУВС, 2018. Вип. 1. С. 283–301.
4. Закон України «Про національну безпеку України» від 21 червня 2018 //Електронний ресурс:<https://zakon.rada.gov.ua/laws/show/2469-19#Text> (дата звернення 08.03.21).