навчальній літературі ми не знайшли. Категорично казати про те, що це питання цілком було виключено з поля зору наукової спільноти не можна. Наприклад, С. О. Кузніченко було з'ясовано, що до адміністративно-запобіжних заходів у змісті надзвичайних адміністративно-правових режимів відносяться особливі правила користування зв'язком і передачею інформації через комп'ютерні мережі [7, с. 21]. С. О. Магда у своєму дослідженні зазначає, що право на інформацію в умовах дії надзвичайних адміністративно-правових режимів набуває особливого значення в ході реалізації уповноваженими органами відповідних заходів, а також у відповідних умовах особливого значення для громадян набувають такі гарантії як належне інформування про реальний стан речей в зоні дії того чи іншого надзвичайного режиму [8, с. 17]. Але ці наукові започаткування та умовиводи не створюють цілковитого комплексного уявлення про зміст та характер змін, які вносяться законами (у зв'язку з введенням того чи іншого особливого правового режиму) до обсягу реалізації права на інформацію.

Необхідно вказати, що зміст надзвичайних (типових та нетипових) адміністративно-правових режимів включає не лише адміністративно-запобіжні заходи та обмеження, а й покладає додаткові обов'язки на спеціальні органи публічного адміністрування. Наприклад, забезпечення населення необхідною інформацією про радіаційний стан території, що зазнала радіоактивного забруднення (*ст. 10 Закону України «Про правовий режим території, що зазнала радіоактивного забруднення внаслідок Чорнобильської катастрофи»*); про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей (*п. 2 ч. 4 ст. 21 Закону України «Про інформацію»*); про вчинення терористичного акту (*ч. 1 ст. 17 Закону України «Про боротьбу з тероризмом»*) тощо. Крім того, потрібно удосконалювати способи забезпечення інформаційних, культурних зв'язків з громадянами України, які проживають на тимчасово окупованій території, у зоні проведення військових дій і т. ін.

Визначення системного переліку заходів та змін, що відбуваються у правовому регулюванні інформаційних правовідносин в умовах уведення надзвичайних (типових та нетипових) правових режимів становить перспективний напрямок наших подальших досліджень.

Література:

1. Манакова И. Ю. Человек в постиндустриальном мире: автореф. дис. … канд. фил. наук: 09.00.11 / Воронеж. гос. ун-т. Воронеж, 2008. 24 с.

2. Дурбас О. П. Розвиток інформаційно-комунікаційного простору в контексті взаємодії культури і політики. *Сучасна українська політика*. 2010. Вип. 19. С. 223–232.

3. Коваленко Л. П. Інформаційне право України. Проблеми становлення та розвитку: дис. … д-ра юрид. наук: 12.00.07 / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2014. 418 с.

4. Рудник Л. І. Право на доступ до інформації: дис. … канд. юрид. наук: 12.00.07 / Нац. ун-т біоресурсів і природокористування Укр. К., 2015. 248 с.

5. Information Security and Privacy in Network Environments. Washington, DC: U.S. Government Printing Office, 1994. 244 p. URL: https://www.princeton.edu/~ota/disk1/1994/9416/941605.PDF (Last accessed: 04.11.2017).

6. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. URL: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046 (Last accessed: 04.11.2017).

7. Кузніченко С.О. Становлення та розвиток інституту надзвичайних адміністративно-правових режимів в Україні: автореф. дис. … д-ра юрид. наук: 12.00.07 / Харків. нац. ун-т внутр. справ. Х., 2010. 34 с.

8. Магда С.О. Забезпечення прав, свобод та реалізації обов'язків громадян в умовах надзвичайних адміністративно-правових режимів: автореф. дис. … канд. юрид. наук: 12.00.07 / Нац. юрид. академія Укр. ім. Ярослава Мудрого. Х., 2008. 22 с.

Головна проблема кібербезпеки: невігластво

Гавриш О.С.
викладач кафедри економічної та інформаційної безпеки
Дніпропетровського державного університету внутрішніх справ

Останнім часом все більше зростає питання захисту програмного забезпечення від зломів. Регулярно з'являються повідомлення про великі витоки даних за підсумками кібератак. У минулому році говорили про кібервикрадення 80 млн. доларів з банку в Бангладеш. Також великою історією стали два витоки даних у Yahoo, що ледь не призвело до зриву продажу Yahoo.

Це тільки деякі прояви діяльності чорного хакерського ринку, на якому продаються викрадені цифрові продукти. У міру поширення цифрових технологій в повсякденному житті проблема буде тільки рости. Якщо раніше в основному крали електронні гроші з електронних рахунків, то тепер до мережі підключається величезна кількість пристроїв, аж до автомобілів. Для хакерів тут відкриваються нові можливості.

Звичайно, противагою цьому може бути зустрічний процес - технологічне вдосконалення захистів. Проблема в тому, що виробники погано мотивовані до впровадження такого роду удосконалень. Вони більше зацікавлені в розробці нових продуктів, що означає більшу кількість коду, що потребує ретельного тестування. В середньому кожен новий програмний продукт налічує 14 вразливостей. Кожна з вразливостей може бути використана для нелегального доступу.

Сучасний комп'ютер, являє собою комбінацію компонентів, що походять з різних джерел - починаючи з комплектуючих і операційних систем і закінчуючи додатками. Кожен з компонентів може містити в собі несправності (допущені помилково або навмисно), які в сукупності створюють вразливість.

Вразливість виникає з основ, на яких стоять інформаційні технології, з культури розробки програмного забезпечення, а також із суперечливих інтересів урядів. Однак зараз бурхливий розвиток кіберзлочинності починає змушувати компанії, уряди і наукові інститути до дій.

Основні тези кібербезпеки сьогодення :

Сучасним атакам практично не можна запобігти, тому зараз не менше зусиль потрібно направляти на підготовку команд реагування на інциденти.

Кіберзлочинці - це не одинаки, це добре підготовлені, добре мотивовані і добре фінансовані організації.

Вся інформація, яку ви знаєте про свою мережу і техніку - ніщо, якщо ви не знаєте, хто вам протистоїть. Тому вам потрібно встати на місце хакера і зрозуміти, що йому може бути цікаво в вашій компанії і як він може це отримати.

Головне порушення кібербезпеки сьогодні - це відсутність комплексного підходу (люди, системи, процеси), ігнорування питань кібербезпеки з боку CEO, зайва впевненість у безпеці.

Раніше зловмисники атакували для шантажу або заволодіння грошовими коштами, сьогодні це використання інфраструктури жертви для атаки на третіх осіб, маніпулювання виборами або техногенні катастрофи.

Кібербезпеку неможливо купити - її можна тільки побудувати.

Всі погоджуються, що актуальність кібератак зростає. До 2007 року кібербезпека фінансувалася за залишковим принципом, тепер ми переходимо в стадію кіберстійкості. Зараз найбільш просунуті програми впроваджують ген кібербезпеки в кожен процес і пристрій, адже навіть кавоварка може бути використана для кібератак.

Кіберризиків як таких не існує - всі вони пов'язані з ризиками втрати грошей, техногенної безпеки тощо. Обсяг світового ринку кібербезпеки за підсумками 2017 року сягне $ 120 млрд. За останні 13 років він виріс в 35 разів.

Література:

1. Проблеми кіберзлочинності [Електронний ресурс]. – Режим доступу: http://kontinentusa.com/kiberbezopasnost-problemy
2. Системный инженер Cisco[Електронний ресурс]. – Режим доступу:https://delo.ua/tech/10-vazhnyh-tezisov-dlja-kiberbezopasnosti-329632/?supdated_new=1510515414

Державне управління у сфері забезпечення кібернетичної безпеки в Україні