СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА
ЛІГА СТУДЕНТІВ АСОЦІАЦІЇ ПРАВНИКІВ УКРАЇНИ

РЕФОРМУВАННЯ ПРАВОВОЇ СИСТЕМИ В КОНТЕКСТІ ЄВРОІНТЕГРАЦІЙНИХ ПРОЦЕСІВ

МАТЕРІАЛИ
IV Міжнародної науково-практичної конференції
(Суми, 21–22 травня 2020 року)

У двох частинах

Частина 2

Суми
Сумський державний університет
2020

ЛІТЕРАТУРА:

1. Про судоустрій та статус суддів: Закон України від 02.06.2016 р. *Відомості Верховної Ради України.* 2016. № 31. Ст. 545.
2. Бояринцева М. А. Адміністративний суд як суб'єкт права. *Науковий вісник Ужгородського національного університету* 2015. Вип. 35, ч. 2, т. 2. С. 71–75.
3. Колпаков В. К., Кузьменко О. В. Адміністративне право України: підручник. Київ: Юрінком Інтер, 2003. 544 с.
4. Бортник В. А. Адміністративне право України: навч. посіб. Київ: ДП «Вид. дім «Персонал». 2012. 222 с.
5. Чернов С. І., Гайдученко С. О. Текст лекцій з дисципліни «Публічне адміністрування» (для студентів всіх форм навчання). Харків: ХНУМГ, 2014. 97 с.
6. Публічне управління : термінол. слов.; за заг. ред. В. С. Куйбіди, М. М. Білинської, О. М. Петроє. Київ: НАДУ, 2018. 224 с.
7. Решота В. Перспективи реформування адміністративної юстиції у системі державного управління України. *Науковий вісник «Демократичне врядування».* 2008. Вип. 1. 7 с.
8. Шевченко Е. О. Визначення поняття адміністративно-правових відносин з урахуванням пріоритетного значення та ролі в них суб'єкта адміністративного права (на прикладі адміністративного суду). *Форум права*. 2011. № 1. С. 1116–1122.
9. Кодекс адміністративного судочинства України від 06.07.2005 р. *Відомості Верховної Ради України.* 2005. № 35–36, № 37. Ст. 446.
10. Селіванов А. О. Адміністративний процес в Україні: реальність і перспективи розвитку правових доктрин. Київ: Видавничий Дім «Ін Юре». 2000. 68 с.
11. Колпаков В. К. Адміністративно-деліктний правовий феномен: монографія. Київ: Юрінком Інтер. 2004. 528 с.
12. Бородін І. Л. Судовий контроль, його співвідношення з адміністративним контролем та прокурорським наглядом. *Науковий вісник Національної академії внутрішніх справ України.* 2002. № 4. С. 171–176.
13. Олендер І. Я. Функції суду в державному механізмі. *Право і суспільство*. 2014. № 1-2. С. 153–158.

КІБЕРАТАКИ ЯК НОВІТНЯ ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Думчиков М.О.
к. ю. н., асистент кафедри КПДС ННІ права
Сумського державного університету

Все частіше в сучасному побуті можна почути термін «кібератаки». Кібератака, у

вузькому сенсі, – це замах на комп'ютерну безпеку інформаційної системи. У широкому ж розумінні, кібератака розглядається як пошук рішень, методів, кінцевою метою яких є отримання контролю над віддаленою системою з метою її дестабілізації.

Стан інформаційної захищеності в області державної та громадської безпеки характеризується постійним підвищенням складності, збільшенням масштабів і зростанням скоординованості комп'ютерних атак на об'єкти критичної інформаційної інфраструктури, посиленням розвідувальної діяльності іноземних держав щодо України, а також наростанням погроз застосування інформаційних технологій з метою нанесення шкоди суверенітету, територіальної цілісності, політичної та соціальної стабільності України. Збиток від хакерських атак, скоєних по всьому світу за останні роки, склав від $ 300 млрд до $ 1 трлн [1].

Розробкою рекомендацій щодо попередження та розслідування інцидентів кібербезпеки займається комп'ютерна криміналістика, активно аналізуючи їх зміст, розробляючи заходи реагування і способи їх попередження. Якщо раніше в традиційне розуміння кібератак входили DOS і DDOS-атаки, то сьогодні кіберзлочинці кардинально поміняли їх зміст.

Наприклад, в травні 2017 р комп'ютерний вірус WannaCry вразив комп'ютерні системи окремих користувачів, комерційних організацій та державних установ по всьому світу. Можливість його поширення зумовили уразливості старих версій операційної системи Windows. WannaCry, проникаючи в систему за допомогою переходу по посиланнях, які містяться в електронних повідомленнях масової розсилки, отримував контроль над нею, зашифровував комп'ютерні файли, після чого на екрані з'являлося повідомлення з вимогою викупу в розмірі 300 доларів США за розшифровку файлів. Викуп необхідно було перерахувати на гаманець Bitcoin. Через 3 дні сума подвоюється і становила 600 доларів США. Через 7 днів зашифровані файли віддалялися безповоротно. За даними міжнародних кіберекспертів Україна в результаті такої кібератаки зазнала найбільшої шкоди: було порушено роботу комп'ютерних систем МВС, МНС, системи вищих навчальних закладів, банківські системи та системи телефонного зв'язку. Ще одна велика кібератака була проведена 27 червня 2017 р Росії і в Україні, зловмисники аналогічним способом масово поширили вірус Petya. Даний вірус-вимагач блокував доступ до даних, вимагаючи за їх розблокування 300 доларів США в Bitcoin.

Представлені приклади є найбільш яскравими і наочно демонструють сутність сучасних кібератак. Узагальнюючи наявні знання про кіберзагрози сучасності можна скласти типову криміналістичну модель кібератак:

- кібератаки можуть здійснюватися як через одного чоловіка, так і групою

хакерів з метою дестабілізації комп'ютерної системи, захоплення контролю над її ресурсами, або відмови в обслуговуванні;

- жертвами кібератак можуть стати як окремі користувачі, так і комерційні організації, державні органи, політичні товариства і навіть цілі держави;
- реалізуються, як правило, віддалено, в зв'язку з чим мають високу латентність. Даний факт здебільшого обумовлений властивостями мережі Інтернет, з одного боку лежать в основі її організації, а, з іншого, забезпечують можливість здійснення таких злочинів;
- умовна анонімність і відсутність єдиного управління обумовлюють складності у виявленні і у встановленні винних у таких злочинних інциденти інформаційної безпеки;
- відстань і транснаціональний характер мережі Інтернет дозволяють проводити кібератаки масштабно, завдаючи максимального збитку;
- способи та методи здійснення кібератак різноманітні: атака листами (спам), фішинг, використання вразливостей.

Причому сучасні тенденції такі, що все більшого поширення набуває проведення кібератак за допомогою розповсюдження шкідливих програм. Таким чином, основним інструментом сучасних кібератак є шкідливе програмне забезпечення. Однак очевидно, що ефективність протидії кібератакам може бути досягнута лише при комплексному підході до вирішення цієї проблеми. Кібератака, на відміну від звичайного поширення вірусів, носить цілеспрямований характер і її мета – конкретна система, з якою працюють певні користувачі, тому захиститися від неї досить складно.

Однак не можна не відзначити роль користувачів комп'ютерних систем в попередженні кібератак, адже багато інцидентів комп'ютерної безпеки стають можливими саме з їхньої вини (використання застарілого програмного забезпечення, перехід на невідомі зовнішні ресурси). Щоб звести до мінімуму ризик кіберзамахів на безпеку комп'ютерної системи користувач повинен дотримуватися елементарних правил кібербезпеки. Ці правила є набором криміналістичних превентивних знань, сформованих на підставі аналізу сучасних інцидентів кібератак [2, с. 17]:

- необхідно використовувати тільки ліцензійне програмне забезпечення з можливістю своєчасного оновлення;
- необхідно стежити за актуальністю антивірусних програм;
- не можна переходити по зовнішнім посиланням, отриманим від невідомих користувачів;
- рекомендується видаляти непрочитаними підозрілі листи від невідомих

користувачів;

- головне правило корпоративної безпеки: один комп'ютер - тільки для роботи з банком, обслуговуючим організацію і більш ні для чого;
- не слід використовувати електронні носії інформації в невідомих пристроях і навпаки.

Якщо комп'ютерна система все-таки була атакована, не поспішати перераховувати грошові кошти зловмисникам, так як немає гарантії того, що шкідливе програмне забезпечення буде безповоротно видалено з комп'ютера і вимагання не повториться знову, а також не приховувати інцидент комп'ютерної безпеки, як від керівництва, так і від правоохоронних органів, не намагатися самостійно перевстановити систему. Необхідно негайно повідомити в правоохоронні органи і вжити всіх заходів для збереження і фіксації слідів здійсненої кібератаки.Дотримання представлених правил захистить комп'ютерну систему конкретного користувача, надасть значну роль у зміцненні інформаційної безпеки України в цілому, а також допоможе в фіксації слідів і в розслідуванні подібних інцидентів.

Незважаючи на всю масштабність кіберзагроз, при узгодженості дій, можливо їм успішно протидіяти. Якщо держава здійснює боротьбу з кіберзлочинцями законодавчими та організаційними заходами, то в силах кожного користувача внести свій неоціненний внесок у спільну справу – знати і дотримуватися елементарних правил кібербезпеки, своєчасно і грамотно реагуючи на неполадки в роботі комп'ютерної системи.

ЛІТЕРАТУРА:

1. Кибератака. URL: http://www.securitylab.ru/news/ (дата звернення: 10.04.2020).
2. Бехметьев А. Е. Кибератаки. *Административное право*. №1. 2017. С. 17.

МЕХАНІЗМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЄВРОПЕЙСЬКОМУ СОЮЗІ ТА ЙОГО ВДОСКОНАЛЕННЯ В УКРАЇНІ

Костенко З. В.
Студент IV курсу ННІ права
Сумського державного університету
Науковий керівник: Думчиков М. О.
к. ю. н., асистент кафедри КПДС ННІ права
Сумського державного університету

У сучасному світі спостерігається широке поширення і застосування інформаційних технологій, методів автоматичної обробки даних, формування глобальних