СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА

РЕФОРМУВАННЯ ПРАВОВОЇ СИСТЕМИ В КОНТЕКСТІ ЄВРОІНТЕГРАЦІЙНИХ ПРОЦЕСІВ

МАТЕРІАЛИ
VI Міжнародної науково-практичної конференції
(Суми, 19–20 травня 2022 року)

Суми
Сумський державний університет
2022

з’явиться більше можливостей на переосмислення свого буття та подальшого успішного життя.

ЛІТЕРАТУРА:

1. Кримінально-виконавчий кодекс України: закон України від 11 березня 2003 р. № 1129-IV. URL: https://zakon.rada.gov.ua/laws/show/1129-15#Text (дата звернення: 06.05.2022).

2. Рощина В. Рівень рецидиву в Україні планують знизити з 30% до 5% — міністр юстиції Малюська про тюремну реформу. Громадське телебачення: веб-сайт. URL: https://bit.ly/3lWlluC (дата звернення: 06.05.2022).

3. Picanço L. Brazil’s Mass Incarceration Policy Has Not Stopped Crime. Wilsom Center : website. URL: https://www.wilsoncenter.org/blog-post/brazils-mass-incarceration-policy-has-not-stopped-crime (дата звернення: 06.05.2022).

4. Castillo M. Brazilian inmates reduce sentences by hitting the bike, books. CCN : website. URL: https://cnn.it/3GBpQUN.

5. Inmates at Brazil prison pedal for electricity - and their freedom. NBC News : website. URL: https://www.nbcnews.com/id/wbna48144469

6. Ромалійська І. Читання книг за крадіжку – таке покарання ухвалив одеський суддя. Що кажуть психологи та юристи? Радіо свобода: веб-сайт. URL: https://www.radiosvoboda.org/a/vyrok-pro-chytannya-knyg-v-odesi/31576441.html (дата звернення: 06.05.2022).

ЗАПОБІГАННЯ КІБЕРЗЛОЧИНАМ ЗА ДОПОМОГОЮ ДОДАТКУ «ДІЯ»

Малетов Д. В.
Доктор філософії з права, викладач-стажист кафедри КПДС ННІ права Сумського державного університету
Печена Т. О.
Студентка ІІ курсу ННІ права Сумського державного університету

Двадцять перше століття безумовно можна назвати ерою цифрових технологій. Бюрократизм змінюється онлайн-операціями, а звичні паперові документи заміщуються зручним електронним варіантом. Таку концепцію називають «Державою в смартфоні». Певна річ, ця система має значну кількість переваг, а в умовах всесвітньої пандемії та війни в України – є необхідним кроком. В ситуації обмеженого пересування громадян країною сплачувати податки, реєструвати документи та здійснювати інші юридичні дії можна просто в один клік.

Разом з розвитком цифрового світу поширюється кіберзлочинність, яка зросла до міжнародних масштабів. Так, за даними спеціалістів компанії McAfee та Центру стратегічних і міжнародних досліджень, загальна кількість витрат від комп'ютерних злодіїв на 2020 рік становила один відсоток від світового ВВП [1]. Найбільш розповсюджені кіберзлочини пов'язані з використанням програм-вірусів, фішингових програм, викрадення інформації з баз даних тощо.

Україна останніми роками дедалі більше відчуває на собі масштаби кібернетичних загроз і їх негативні наслідки. Станом на 2020 рік Національна поліція України викрила понад 5000 кіберзлочинів. «Шахрайства з платіжними картками, крадіжки грошей з банківських рахунків, розповсюдження комп'ютерних вірусів, викрадення хакерами персональних даних громадян, онлайн-торгівля наркотиками, протидія піратству та поширенню протиправного контенту - це далеко не повний перелік завдань Кіберполіції. Загалом минулого року було зареєстровано понад 5 000 кіберзлочинів, в яких вдалося оперативно затримати 106 фігурантів кримінальних проваджень, серед яких - 13 педофілів», - розповів Ігор Клименко [2].

Розслідувались такі категорії злочинів у сфері використання електронних обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, відповідальність за які встановлена статтями 16 розділу особливої частини Кримінального кодексу України, як: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; створення з метою використання, розповсюдження або збуту шкідливих програм чи технічних засобів, а також їх розповсюдження або збут тощо [3].

Збільшення кібернетичних атак в Україні безпосередньо пов'язано із запровадженням вищезгаданої концепції та її активного розвитку. Для плодотворної роботи «Держави в смартфоні» необхідно багато персональних даних помістити в бази або додатки. Саме тому в 2019 році було презентовано мобільний додаток «Дія», основною функцією якого є зберігання найважливіших документів та реалізація юридичних дій в простому електронному форматі. При цьому, всі правочини, що здійснюються через програму мають таку саму юридичну силу, що і паперові варіанти. Таким чином, Україна стала першою державою в світі електронний паспорт якої має таке саме вагоме значення, як і його класичний друкований вигляд. Юридично закріплено це було внесенням змін до Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують її особу або спеціальний статус». Так, статтю 3 доповнили пунктами такого змісту: «Е-паспорт - паспорт громадянина України у формі електронного відображення інформації, що

міститься у паспорті громадянина України у формі картки, оформленому засобами Реєстру, разом з унікальним електронним ідентифікатором (QR-кодом, штрих-кодом, цифровим кодом), а також інформації про місце проживання (за наявності); е-паспорт для виїзду за кордон - паспорт громадянина України для виїзду за кордон у формі електронного відображення інформації, що міститься у паспорті громадянина України для виїзду за кордон, оформленому засобами Реєстру, разом з унікальним електронним ідентифікатором (QR-кодом, штрих-кодом, цифровим кодом), а також інформації про місце проживання та податковий номер (реєстраційний номер облікової картки платників податків з Державного реєстру фізичних осіб - платників податків) (за наявності)"; надає кваліфіковані електронні довірчі послуги в установленому законодавством порядку"[4].

Окрім усіх вищевказаних переваг «Держави в смартфоні» мобільний додаток «Дія» допомагає попереджати кіберзлочини, адже один з його сервісів направлений на боротьбу з цифровими аферами. Мова йде про пуш-сповіщення щодо перевірки чи зміни кредитної історії з Українським бюро кредитних історій. Тому підтвердженням є випадок, що стався в січні цього року: на своєму аккаунті Facebook користувачка додатку поширила допис про спробу зловмисників взяти на її ім’я декілька мікрокредитів, про що вона дізналася за допомогою механізму сповіщень. Зловмисники перевипустили SIM-карту з номером потерпілої. Ця карта не була прив’язана до паспорта, що дало змогу отримати доступ до мобільного банкінгу, а також оформити мікрокредити в декількох установах, а саме "Манівео", "Форза", "Швидкозайм". Завдяки новому сервісу потерпіла одразу дізналася про здійснене правопорушення та оперативно на нього відреагувала. Водночас через скомпрометований BankID зловмисник авторизувався у "Дії", що було одразу зафіксовано в застосунку в розділі “активні сесії”. За цим фактом кіберполіцією розпочато відповідне розслідування.

Жодних дій із застосунком та документами потерпілої зловмисники не вчинили та не могли вчинити навіть теоретично через відповідну безпекову модель роботи "Дії". Адже цифрові документи надійно захищені. І для того, щоб оформити кредит з цифровим документом в застосунку, потрібен цифровий підпис. Це технологія, яка у режимі реального часу порівнює біометрію обличчя з фотографією у реєстрі. Для шерингу документів також потрібен "Дія-підпис", який неможливо підробити без біометрії обличчя.

У цьому випадку "Дія" допомогла дівчині зупинити шахрайську схему та захистити кошти. Якби сповіщення не було, то вона не змогла б так швидко дізнатися про шахраїв та оперативно відреагувати. [5]

Після дослідження проблематики протидії кіберзлочинності постає питання щодо відповідальності за завданні злочини. У чинному Кримінальному кодексі наявний «спеціалізований» розділ, який визначає відповідальність за кіберзлочини: розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», який складається із 6 статей:

- ст. 361 – несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;
- ст. 361-1 – створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут;
- ст. 361-2 – несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;
- ст. 362 – несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї;
- ст. 363 – порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється;
- ст. 363-1 – перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку [3].

В основному відповідальність за перелічені правопорушення передбачає накладання штрафу, або, у повторювальних випадках, позбавлення волі на певний строк.

Варто додати, що об'єкти кібербезпеки та кіберзахисту зазначені в статті 4 Закону України «Про основні засади забезпечення кібербезпеки України», до яких відносяться:

- конституційні права і свободи людини і громадянина;
- суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;
- держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

- національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;
- об’єкти критичної інфраструктури;
- комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;
- об’єкти критичної інформаційної інфраструктури;
- комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу[6].

Попри достатньо конструктивний нормативно-правовий аспект протидії кіберзлочинності вважаю необхідним розвиток правового регулювання злочинів, вчинених саме за допомогою «Дії». Хоч Мінцифри і завірює, що витік даних з мобільного додатку неможливий, подібні випадки, як розглянутий нами, існують. Чинне законодавство, як на мене, є дещо застарілим як для таких новітніх технологій, як «Держава у смартфоні» через що потребує окремої уваги.

Осягання актуальної інформаційно-правової проблематики боротьби з кіберзлочинністю, та можливостей її зменшення, підвищить ефективність розслідування кіберзлочинів органами правопорядку України. Тому є необхідність деталізації законодавства, яке б відображало дійсну ситуацію із існуючими загрозами кримінальних правопорушень у цифровій сфері, впровадження механізмів сприяння правоохоронним органам України операторів, провайдерів щодо забезпечення належної електронної бази даних, лімітування доступу абонентів до інформаційного ресурсу (інформаційного сервісу) тощо.

Основуючись на вищевикладеному, вбачаємо багатообіцяючою можливістю превенції та розслідування кіберзлочинів постійне підвищення кваліфікації задіяних співробітників правоохоронних органів з метою вивчення існуючих варіантів тактики проведення слідчих дій для отримання електронних доказів [7].

ЛІТЕРАТУРА:

1. Center for Strategic and International Studies Режим доступу: https://www.csis.org/.
2. Офіційний сайт Національної поліції: веб-сайт. URL: https://bit.ly/3lYZF1a.
3. Кримінальний Кодекс України: Кодекс України; Кодекс, Закон від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

4. Закон України: Про внесення змін до Закону України "Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус". Відомості Верховної Ради (ВВР), 2021, № 27, ст.224). URL: https://zakon.rada.gov.ua/laws/show/1368-20#Text.
5. Мінцифри розповідає, як у "Дії" борються з шахрайством: веб-сайт. URL: https://bit.ly/38RyylL.
6. Закон України: Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19/conv#n49.
7. Марущак А. І. Інформаційно-правові аспекти протидії кіберзлочинності. “Інформація і право” № 1 (24) / 2018, с. 127-132.

ВІКТИМОЛОГІЧНІ ЧИННИКИ ДОМАШНЬОГО НАСИЛЬСТВА В УКРАЇНІ

Мартинець І. В.
здобувачка вищої освіти
Навчально-наукового інституту права та інноваційної освіти
Дніпропетровського державного університету внутрішніх справ
Науковий керівник: Сенько В. В.
викладач кафедри кримінально-правових дисциплін
Дніпропетровський державний університет внутрішніх справ

Під домашнім насильством розуміють усі акти фізичного, сексуального, психологічного чи економічного насильства, які відбуваються у сім'ї чи побуті між колишнім чи нинішнім подружжям чи партнерами. Домашнє насильство – це модель поведінки, яка використовується однією людиною для контролю або домінування над іншою, з якою вона має або були інтимні або сімейні відносини. Домашнє насильство – це цикл, що повторюється зі збільшенням частоти: фізичної, словесної, духовної та економічної образи з метою контролю, залякування, навіювання почуття страху.

Актуальність даної теми полягає в тому, що домашнє насильство стало розглядатися як соціальна проблема нещодавно й отримало негативну оцінку з боку суспільства. Особа, яка зазнає насильства, перебуває під впливом наслідків насильства, що випливає з різних чинників домашнього насильства. Наслідками можуть бути погіршення здоров'я, психічного стану, зміна поведінки жертви як члена суспільства на гірший бік, через що страждають і професійні якості та відносини з іншими людьми. Потерпілий, несучи у собі весь тягар негативних емоційних переживань і внаслідок погіршення її здоров'я, неспроможна повністю реалізувати себе у різних сферах своєї