

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ
ХЕРСОНСЬКИЙ ФАКУЛЬТЕТ
КАФЕДРА ПРОФЕСІЙНИХ ТА СПЕЦІАЛЬНИХ ДИСЦИПЛІН**



**ПРІОРИТЕТНІ НАПРЯМКИ
РЕФОРМУВАННЯ ПРАВОВОЇ СИСТЕМИ
УКРАЇНИ
В УМОВАХ ВОЄННОГО СТАНУ**

*матеріали Всеукраїнської науково-практичної
конференції
19 жовтня 2022 року*

Одеса
2022

ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ХЕРСОНСЬКИЙ ФАКУЛЬТЕТ

КАФЕДРА ПРОФЕСІЙНИХ ТА СПЕЦІАЛЬНИХ ДИСЦИПЛІН

**ПРІОРИТЕТНІ НАПРЯМКИ РЕФОРМУВАННЯ
ПРАВОВОЇ СИСТЕМИ УКРАЇНИ
В УМОВАХ ВОЄННОГО СТАНУ**

матеріали Всеукраїнської науково-практичної конференції
19 жовтня 2022 року

Одеса
2022

Відповідальний редактор – доктор юридичних наук, професор, завідувач кафедри професійних та спеціальних дисциплін Херсонського факультету Одеського державного університету внутрішніх справ **Шкута О. О.**

Матеріали друкуються в авторській редакції. Відповідальність за дотримання академічної доброчесності, відповідності фактів, цитат, прізвищ тощо несуть автори

Пріоритетні напрямки реформування правової системи України в умовах воєнного стану: матеріали Всеукраїнської науково-практичної конференції (м. Одеса, 19 жовтня 2022 р.) / за ред. д. ю .н. Шкути О.О. – Одеса: Херсонський факультет Одеського державного університету внутрішніх справ, 2022. – 209 с.

До збірника увійшли тези доповідей, подані учасниками Всеукраїнської науково-практичної конференції «Пріоритетні напрямки реформування правової системи України в умовах воєнного стану», які присвячені міжнародним та національним аспектам реформування сучасних напрямків розвитку правової системи України в умовах воєнного стану.

Борисова К.Є., Світличний В.А. ГАДЖЕТИ ЯК НЕБЕЗПЕКА, ДЖЕРЕЛО ІНФОРМАЦІЇ ДЛЯ ВОРОГА. «КІБЕРГІГІЕНА» У ВОЄННИЙ ЧАС	91
Борматов Р.С., Світличний В.А. «КІБЕРГІГІЕНА» В УМОВАХ ВОЄННОГО СТАНУ	93
Верзілов М.Р., Світличний В.А. ЗЛОМ ВЕБКАМЕР АБО КАМФЕКТІНГ	94
Виглазов В.С., Світличний В.А. КІБЕРБЕЗПЕКА ПІД ЧАС ВІЙНИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ.....	96
Вдовиченко О.М. КРИМІНОЛОГІЧНІ АСПЕКТИ КІБЕРЗЛОЧИННОСТІ В СУЧАСНИХ УМОВАХ ВОЄННОГО СТАНУ	97
Володько В.О., Світличний В.А. ПРОБЛЕМИ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ЩОДО ПОРУШЕННЯ АВТОРСЬКОГО ПРАВА НА КОМП'ЮТЕРНІ ПРОГРАМИ.....	100
Глушенко І.О., Світличний В.А. ЯК ЗАБЕЗПЕЧИТИ БЕЗПЕКУ СВОЇХ ОСОБИСТИХ ДАНИХ ТА ГАДЖЕТІВ	102
Гордієнко Д.С., Калякін С.В. ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ВІД DOS-АТАК ПІД ЧАС ВОЄННОГО СТАНУ	105
Грон М.С., Калякін С.В. БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ В УМОВАХ ДІЇ ВОЄННОГО СТАНУ: ЗАКОН 2149-ІХ	108
Груба В.В., Калякін С.В. БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ В УМОВАХ ДІЇ ВОЄННОГО СТАНУ	111
Груздова В.О. Колошко Ю.В. ВІРТУАЛЬНІ КОМУНІКАЦІЇ В ЖИТТІ СУЧАСНОЇ МОЛОДІ	116
Гупалюк Я. Р., Світличний В.А. БІОМЕТРІЯ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В УМОВАХ ВОЄННОГО СТАНУ	118
Дзярик В.М., Калякін С.В. КІБЕРГІГІЕНА	120
Донець Я.О., Світличний В.А. КІБЕРБЕЗПЕКА У ВОЄННИЙ ЧАС	121
Дубина В.Є., Світличний В.А. ЗАХИСТ ІНФОРМАЦІЇ ПІД ЧАС ВОЄННОГО СТАНУ	123
Єрьоменко Я.С., Онищенко Ю.М. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ, СТВОРЕНІ КУРСАНТАМИ ХНУВС ДЛЯ ЗАПОБІГАННЯ ТА ПРОТИДІЇ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ.....	125

Вдовиченко Олексій Маратович

доцент кафедри адміністративної діяльності поліції Одеського державного університету внутрішніх справ, доктор філософії

КРИМІНОЛОГІЧНІ АСПЕКТИ КІБЕРЗЛОЧИННОСТІ В СУЧАСНИХ УМОВАХ ВОЄННОГО СТАНУ

Реалії сьогодення все частіше підштовхують людство до процесів глобалізації і тому активне застосування комп'ютерних технологій у всіх значимих сферах життя суспільства є невід'ємною характеристикою сучасного миру та складовою невід'ємної частини життя. Вимкнення Інтернету на добу є такою ж, а може і більшою, проблемою для людини, як відключення електроживлення, чи водопостачання особливо в тих умовах які виникли на сьогодення, а саме воєнний стан, в таких умовах і зростає більшість кримінальних правопорушень у сфері кіберзлочинності.

Існування так званих гаджетів у життєдіяльності людини розширює можливості, надає багато додаткових механізмів і способів її реалізації, зокрема уникнути від зайвого багажу витрат, пришвидшує процес обміну інформації, і як наслідок є невід'ємним інструментом отримання прибутку. Однак такі додаткові можливості не завжди використовуються в законних цілях.

Суспільна небезпека кримінальних правопорушень у сфері комп'ютерної інформації полягає в тому, що неправомірний доступ або зміна комп'ютерної інформації може порушувати діяльність різних систем забезпечення держави: оборони, енергетики, транспорту та спричинити не тільки матеріальний збиток, але і людські жертви [1, с. 109].

Такі комп'ютерні кримінальні правопорушення є однією з активних груп суспільно небезпечних посягань. Достатньо швидко зростають показники поширення цих кримінальних правопорушень, а також постійно зростає їх суспільна небезпечність. Така ситуація зумовлюється прискореним розвитком сучасних технологій в ІТ-сфері, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки.

Історією неодноразово повчалися, що розвиток і прогрес, які приносять людям нові блага та можливості, на жаль, завжди супроводжуються негативними явищами. Індустріалізація дала нам масове виробництво товарів, але вона ж поклала початок варварському винищенню природи і класовій нерівності. Боротьба за національні та соціальні права зробила аксіомою принципи рівності і справедливості, але часто призводить до кровопролиття і негативних проявів патерналізму [2].

Основною метою вчинення кіберзлочину є широкий спектр варіантів. Для активних кіберзлочинців це переважно насильницька мотивація, що обумовлена психоемоційними розладами сексуального характеру та нав'язливими ідеями. Для пасивної категорії – збагатитися, самоствердитися проявити творчі здібності або звичайна цікавість поєднана із зухвалістю. Можемо визначити, що Кіберпростір і в мирний час насичений шкідливим програмним забезпеченням та кіберзлочинцями, а у воєнний час ця небезпека анітрохи не зменшилася. В умовах сучасної гібридної війни, яка відбувається в інформаційному та кіберпросторі, загроза онлайн-атак тільки зросла.

Набагато складніше визначити місце вчинення комп'ютерного злочину. Більшість злочинів у сфері комп'ютерної інформації відбувається в комп'ютерних мережах. Це передбачає, що місце вчинення протиправного діяння і місце настання суспільно небезпечних наслідків можуть відділятися один від одного багатьма кілометрами і навіть перебувати на території різних держав [3, с. 14].

Слід зазначити що, від початку війни в Україні активізувався неофіційний громадський рух кіберопору ворогові. Звичайні люди, поряд із професіоналами сфери ІТ, наносять нищівний удар атакуючи ворога у кіберпросторі, завдають йому збитків та зривають плани.

Абсолютно всі користувачі інтернету є учасниками кіберпростору. І не важливо, чи ви програмуєте, сплачуєте комунальні послуги або просто читаете новини. Як тільки ви зайшли у мережу інтернет, ви вже один з жителів кіберпростору з відповідними правами та небезпеками. Загрози стало важче відстежити.

Семенов В.М. та Гиркіна О.О. звертають увагу на те, що сучасні інформаційні технології перетворюють інформаційні системи урядового, оборонного,

виробничого, кредитно-банківського, комунального та інших секторів на надзвичайно вразливі для реалізації кіберзагроз об'єкти [4, с. 235].

Однією з особливостей боротьби з кіберзлочинністю в умовах воєнного стану є те, що з метою недопущення зростання великого рівня кіберзлочинності було прийняті певні зміни до чинного законодавства щодо підвищення боротьби з кіберзлочинністю яке включало посилення відповідальності за несанкціоноване втручання в роботу електронних систем.

Тоді коли метою таких дій є розкрадання або руйнування інформації в інформаційних системах і мережах а також в умовах війни кіберзлочини можуть здійснюватися з метою дестабілізації ситуації в країні, крадіжки необхідних (конфіденційних) даних, виведення з ладу державних інституцій, техніки, завдання іншої матеріальної шкоди.

Отже забезпечення кібербезпеки в умовах воєнного стану є одним із першочергових завдань, що стоїть перед державою, побудову власної законодавчої системи, у тому числі через врегулювання правовідносин шляхом прийняття спеціального закону; внесення змін до кримінального законодавства за для «заповнення» існуючих колізій, прогалин і приведення у відповідність з міжнародними стандартами; забезпечення додержання національної стратегії з кібербезпеки, постійне доповнення її відповідними заходами; організацію систематичного широкомасштабного інформування населення про загрози, що можуть мати місце при використанні сервісів Інтернет.

Список використаних джерел:

1. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: дис. ... канд. юрид. наук: 12.00.08. - Иркутск, 2008. - С. 269.
2. Довбиш М. Кіберзлочинність в Україні. URL: <https://www.science-community.org/uk/node/16132>
3. Рассолов И.М. Киберпреступность: понятие, основные черты, формы проявления / И.М. Рассолов // Юридический мир. - 2008. - № 2. - 152 с.
4. Семенов В.М., Гиркіна О.О. Сучасні аспекти забезпечення інформаційної безпеки України. Науковий вісник Херсонського державного університету: Серія: Юридичні науки. Вип. 5., Т. 2. С. 235.