УДК 343.533:004:342.98
DOI https://doi.org/10.32782/2307-1745.2023.66.30

Гресь Ю. О.,
кандидат юридичних наук, доцент,
доцент кафедри криміналістики, детективної та оперативно-розшукової діяльності
Національного університету «Одеська юридична академія»

КІБЕРЗЛОЧИНИ СЛУЖБОВИХ ОСІБ: РИЗИКИ, ВИДИ ТА КРИМІНАЛІСТИЧНІ ЗАСОБИ ПРОФІЛАКТИКИ

Анотація. У статті досліджено окремі особливості вчинення кіберзлочинів службовими особами. Службова злочинність становить собою значну загрозу для суспільства та нормального функціонування правової держави. Дане поняття об'єднує значну кількість передбачених Кримінальним кодексом України караних діянь. Службові злочини характеризуються високим рівнем латентності та пов'язані із порушенням довіри громадян до державних інституцій, підривом нормального функціонування правоохоронної системи та створюють загрозу для ефективного здійснення державного управління. Побудова цифрової держави в України відкриває нові можливості для розвитку суспільства, але разом із тим створює нове поле для здійснення злочинних посягань.

У статті проаналізовано основні ризики вчинення кіберзлочинів у сфері професійної діяльності службових осіб. Визначено, що такі процеси, як цифровізація суспільства в умовах відсутності інформаційної грамотності державних службовців, накопичення значних масивів інформації у базах даних, низький рівень правосвідомості службових осіб, економічна криза, значний рівень корумпованості службової діяльності, безпекові недоліки та прогалини захисту систем безпеки баз даних, невідповідність рівня знань та вмінь службових осіб їх заробітній платі, а також недосконала система кримінально-правової охорони обумовлюють підвищення ризиків учинення кіберзлочинів у сфері службової діяльності.

Крім того, наведено деякі види кіберзлочинів, що можуть вчинятися службовими особами, зокрема несанкціонований доступ до інформації інтимного змісту, зловживання службовими повноваженнями з метою заволодіння інформацією стратегічного змісту чи заволодіння або використання технічних ресурсів, маніпулювання даними та документами, зловживання технічним обладнанням, знищення або зміна доказів.

Запропоновано систему певних засобів криміналістичного попередження та протидії вчинення кіберзлочинів службовими особами, серед яких: контроль за доступом, моніторинг активності, захист інформації, створення політики безпеки, аудит безпеки та користувачів, здійснення резервного копіювання даних та історії їх зміни, попередження про кримінальну відповідальність.

Ключові слова: злочини у сфері службової діяльності, службова особа, досудове розслідування, корупційні злочини, співробітники правоохоронних органів, кіберзлочини, кібербезпека, криміналістична методика розслідування злочинів, криміналістична профілактика, криміналістичне попередження та протидія злочинності.

Постановка проблеми. Розділ XVII Кримінального кодексу України передбачає цілу низку кримінальних правопорушень, що вчиняють у сфері службової діяльності [1]. У межах наук кримінально-правового циклу, науковці, які займалися дослідженням даної тематики, підкреслюють значну суспільну небезпечність такого прояву злочинності та наголошують на шкоді, що завдається правам та законним інтересам окремих громадян, юридичним особам, державі та її органам. В.Є. Бондар зазначає, що злочинність службових осіб, пов'язана із їх професійною діяльність, поглиблює суспільні кризові явища, провокує виникнення нових загроз та шкодить іміджу України на світовій арені [2, с. 145]. Д.Г. Михайленко акцентує увагу на тому, що злочини у сфері службової діяльності посягають на інституційну безпеку держави, яка є важливою складової національної безпеки країни [3, с. 378]. Значна суспільна небезпечність даної категорії злочинних діянь обумовлюється, також, високим рівнем їх латентності [4, с. 86] та корупційною складовою [5]. Крім того, останні тенденції цифровізації суспільства мають свій вплив і на сферу надання публічних послуг, що призводить до зростання кількості вчинення службових кримінальних правопорушень, які супроводжуються використанням інформаційних технологій та моделей, які впроваджені в економіку та інші сфери за рахунок посилених процесів цифровізації.

Аналіз останніх досліджень і публікацій. До питання сутності службової злочинності та особливостей розслідування її проявів зверталися у своїх роботах такі вчені, як Л.І. Аркуша, В.Є. Бондар, О.В. Вахрушев, А.Ф. Волобуєв, О.О. Дудоров, В.А. Журавель, В.О. Коновалова, В.О. Малярова, Г.А. Матусовський, М.А. Погорецький, О.О. Пунда, О.В. Пчеліна, О.І. Ромців, Д.Б. Сергєєва, Д.М. Стародуб, Р.Л. Степанюк, Є.Л. Стрєльцов, В.Ю. Шепітько, Б.В. Щур та деякі інші. Наукові роботи зазначених вчених містять положення, що стосуються видів та способів вчинення злочинів службовими особа, окремих особливостей розслідування даних видів злочинної діяльності, використання тактичних, техніко-криміналістичних засобів, використання спеціальних знань тощо. Проте основна увага приділяється традиційним способам злочинної діяльності. В той же час окремого наукового криміналістичного опрацювання, на нашу думку, заслуговує питання, що пов'язане зі специфікою вчинення злочинів у сфері злочинної діяльності, обумовленою тенденцією формування в Україні цифрової держави. Є кремі наукові публікації з даного приводу [6], проте повноцінні дисертаційні дослідження даної тематики на разі відсутні.

Мета статті полягає у дослідженні ризиків вчинення кіберзлочинів службовими особами у зв'язку із виконанням ними своїх повноважень відповідно до займаних посад, безпосередньо самих видів кіберзлочинів, що вчиняються такими особами, а також визначення можливих засобів криміналістич-

ної профілактики задля попередження та протидії таким проявам злочинної діяльності службових осіб.

Виклад основного матеріалу. Визначення сутності та видів кіберзлочинів службових осіб, в першу чергу, вимагає розуміння того, що слід розуміти під кіберзлочинами у цілому. Вітчизняне законодавство визначає кіберзлочини як суспільно небезпечні винні діяння у кіберпросторі та/або з його використанням, відповідальність за які передбачена законом України про кримінальну відповідальність та/або яке визнано злочинами міжнародними договорами України [7]. О.А. Самойленко, аналізуючи міжнародні нормативно-правові акти, присвячені кіберзлочинам, дійшла до висновку, що на міжнародній арені дане поняття досить виправдано використовується для позначення усіх традиційних злочинів, вчинених у кіберпросторі [8, с. 58]. Тому можна погодитися із твердженням, що під кіберзлочинами слід розуміти протиправні винні діяння, що вчиняються у формі дії або бездіяльності, які передбачають втручання в дані персональних комп'ютерів, комп'ютерних програм і комп'ютерних мереж, або діяння, вчинені за допомогою комп'ютерів та інших сучасних технологій, за які передбачається кримінальна відповідальність та які можуть створювати особисту небезпеку для громадян, загрозу національній безпеці держави та світовій безпеці у цілому [9, с. 75]. Єдине уточнення може стосуватися того, що до кіберзлочинів слід відносити усі кримінально карані діяння, вчинення яких передбачає використання на певному етами реалізації злочинного умислу можливостей кіберпростору.

Тож зазначимо, що необхідність дослідження певних злочинів, що вчиняються у сфері службової діяльності, саме з позиції визначення їх як кіберзлочинів, обумовлена специфікою способу та обстановки їх учинення. А саме застосуванням певного комп'ютерного обладнання та програмного забезпечення, доступом до цифрової інформації та здійсненням протиправних дій по відношенню до неї за рахунок використання свого службового становища.

Ризики вчинення кіберзлочинів службовими особами становлять собою комплексну систему, що детермінується соціально-економічними факторами, етично-культурними та моральними цінностями, рівнем професійної правосвідомості та деформації осіб, а також загальною стратегією та конкретними кримінально-правовими заходами попередження, протидії та примусу. Серед основних ризиків вчинення кіберзлочинів у сфері професійної діяльності службових осіб, на нашу думку, слід визначити наступні:

1. Стрімкий розвиток процесу цифровізації суспільства у цілому та переведення окремих державних інститутів у цифрове поле в умовах відсутності державної програми інформаційної грамотності державних службовців та посадових осіб центральних органів виконавчої влади та органів місцевого самоврядування.

2. Накопичення значних обсягів особистої інформації у державних базах даних.

3. Недостатній рівень правосвідомості службових осіб органів державної влади та органів місцевого самоврядування.

4. Негативний вплив економічної кризи та ескалації збройного конфлікту між Україною та Російською Федерацією на фінансове та майнове становище значної частини українського суспільства, в тому числі – осіб, наділених певними владними, організаційно-управлінськими чи розпорядчими повноваженнями відповідно до їх службових повноважень.

5. Значні корупційні ризики службової діяльності представників різних органів та установ.

6. Недоліки у існуючих системах безпеки баз даних, що пов'язані із наявністю слабких місць у внутрішніх системах безпеки. Така ситуація створює можливості для вчинення кіберзлочинів службовими особами, які мають до них доступ.

7. Невідповідність високого рівню технічних знань та компетенції службових осіб, особливо, що стосується співробітників правоохоронних органів, офіційному розміру фінансової винагороди, що провокує даних осіб використовувати свої навички для злочинних дій у кіберпросторі.

8. Існування розбіжностей визначення кіберзлочинів, кіберзлочинності та кібербезпеки у міжнародному та вітчизняному законодавстві, що призводить до виникнення складнощів не лише із кваліфікацією певних протиправних діянь, але й до вибору засобів та способів їх попередження, профілактики, виявлення, припинення та якісного розслідування.

Аналізуючи зазначені ризики, а також наукові дослідження, присвячені злочинності у сфері службової діяльності та практику діяльності з розкриття та розслідування злочинів, на нашу думку, можна визначити наступні види кіберзлочинів службових осіб:

1. *Несанкціонований доступ до інформації інтимного змісту*. Співробітники з високим рівнем доступу до конфіденційної інформації можуть вчиняти кіберзлочини, отримуючи несанкціонований доступ та використовуючи цю інформацію в особистих або злочинних цілях. Особливо це стосується співробітників правоохоронних органів, які мають можливість проведення негласних слідчих (розшукових) дій, пов'язаних із втручанням у приватне спілкування, та певних оперативно-розшукових заходів.

2. *Зловживання службовими повноваженнями з метою заволодіння інформацією стратегічного змісту чи заволодіння або використання технічних ресурсів.* Службові особи можуть використовувати свої повноваження для вчинення кіберзлочинів, таких як крадіжка даних в особистих цілях чи з метою отримання неправомірної вигоди в результаті її передачі зацікавленим особам. Крім того, службові особи в силу виконання своїх управлінських чи організаційно-розпорядчих повноважень можуть вчиняти протиправні дії, пов'язані з використанням технічних ресурсів або програмного забезпечення в особистих інтересах.

3. *Маніпулювання даними та документами.* Службові особи можуть використовувати свій доступ для вчинення операцій з базами даних щодо пошук, ознайомлення, оновлення, додавання та стирання цілих записів чи їх частин, документів з метою отримання матеріальної чи іншої вигоди, або створення перешкод для роботи з цією інформацією.

4. *Зловживання технічним обладнанням.* Співробітники з доступом до технічних систем можуть використовувати свої навички для вчинення кібератак, завдання шкоди інформаційним системам безпосередньо за місцем їх роботи, або ж щодо інформаційних систем вітчизняних чи іноземних державних або приватних органів та установ.

5. *Знищення або зміна доказів.* Співробітники правоохоронних органів можуть вчиняти дії, спрямовані на знищення або зміну цифрових доказів. Також державні службовців та

посадові особи центральних органів виконавчої влади та органів місцевого самоврядування можуть вживати заходів, спрямованих на знищення або зміну цифрових доказів, щоб приховати вчинення ними інших незаконних та уникнути відповідальності.

Висновки і пропозиції. З урахуванням зазначеного важливим, на нашу думку, є визначення системи засобів криміналістичної профілактики з метою попередження та протидії таким проявам злочинної діяльності службових осіб, що мають ознаки кіберзлочинів. Зазвичай криміналістичну профілактику розглядають як один із напрямів криміналістичної науки, що спрямований на розроблення рекомендацій та засобів усунення або нейтралізації причин й умов вчинення кримінального правопорушення та здійснює попереджувальний вплив на осіб, які мають схильність до їх учинення. [10, с. 67]. За своєю сутністю це інтегрована система, створена задля забезпечення боротьби зі злочинністю [11, с. 213] шляхом поєднання технік-криміналістичних, тактичних та методико-криміналістичних засобів, організаційних заходів, правових механізмів та освітніх державних програм.

На нашу думку, серед засобів криміналістичного попередження та протидії вчинення кіберзлочинів службовими особами, можна визначити наступні:

1. Контроль за доступом. Обмеження доступу службових осіб до конфіденційної інформації лише до того рівня, який необхідний для виконання їхніх обов'язків, може зменшити ризик неправомірного використання повноважень.

2. Моніторинг активності. Регулярний моніторинг дій та активності співробітників в інформаційних системах може виявити незвичайні або підозрілі зміни, що може бути ознакою можливої кіберзлочинності. Крім того збереження результатів моніторингу активності дозволить ідентифікувати певну особу, що отримувала доступ до конкретної інформації, у випадку відкриття кримінального провадження, яке стосується даної інформації.

3. Захист інформації. Використання шифрування, механізмів аутентифікації та інших технічних засобів захисту допомагає убезпечити конфіденційні дані від несанкціонованого доступу.

4. Створення політики безпеки. Визначення чіткої політик безпеки та їх впровадження допомагає створити стійке середовище безпеки для усіх співробітників.

5. Аудит безпеки та користувачів. Проведення систематичних аудитів безпеки дозволяє виявляти слабкі місця та покращувати заходи безпеки відповідно до змін у загрозах та технологіях. Аудит користувачів дозволить виявити закономірності здійснення доступу до конкретної інформації чи певних її видів з метою подальшого з'ясування причин такого доступу та виявлення можливого вчинення протиправних дій.

6. Здійснення резервного копіювання даних та історії їх зміни. Регулярне створення та зберігання резервних копій даних спрямоване на забезпечення можливості їх відновлення після атаки або втрати. Крім того збереження історії змін є важливим з позиції аналізу цих змін за умови необхідності визначення конкретного моменту вчинення неправомірних дій щодо даної інформації.

7. Попередження про кримінальну відповідальність. Системне роз'яснення міри та виду відповідальності за втручання у роботу інформаційних систем та баз даних службовими особами дозволить попередити вчинення такими особами кіберзлочинів через побоювання настання конкретних наслідків.

Перелік даних заходів не є вичерпним та може бути доповнений в силу того, що діяльність різних видів осіб та вчинювані ними кіберзлочини будуть відрізнятися професіоналізмом їх учинення, характером та змістом дій, а також результатами та наслідками їх учинення.

Література:

1. Кримінальний кодекс України: Закон України від 5 квітня 2001 року № 2341-III URL: https://zakon.rada.gov.ua/laws/show/2341-14.
2. Бондар В.Є. Кримінологічна характеристика злочинів у сфері службової діяльності працівників правоохоронних органів. *Науковий вісник Національної академії внутрішніх справ.* 2016. № 2 (99). С. 145-156.
3. Михайленко Д. Г. Загальні властивості злочинів у сфері службової діяльності та професійної діяльності, пов'язаної з наданням публічних послуг. *Сучасне кримінальне право України: наукові нариси : монографія* / за ред. Н. А. Мирошниченко, Є. Л. Стрельцова; передмова С. В. Ківалова. Одеса : Юридична література, 2017. С. 378-400. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/9286/4.pdf?sequence=1&isAllowed=y
4. Пчеліна О.В. Поняття злочинів у сфері службової діяльності. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція.* 2014. № 10-1. Том 2. С. 86-89.
5. Суворов О. М. Поняття службових злочинів корупційної спрямованості та їх криміналістична характеристика. *Часопис Академії адвокатури України.* 2014. Т. 7. № 4. С. 66-71.
6. Вейц А.М. Характеристика службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг, яка вчиняє кіберзлочин. *Наукові перспективи.* 2023. № 5 (35). С. 554-565.
7. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 23.09.2023).
8. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія / за заг. ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с.
9. Русецький А.А., Куцолабський Д.А. Теоретико-правовий аналіз понять «кіберзлочин» і «кіберзлочинність». *Право і безпека.* 2017. № 1 (64). С. 74-78.
10. Криміналістика: підруч. для студ. вищ. навч. закл. / К. О. Чаплинський, О. В. Лускатов, І. В. Пиріг, В. М. Плетенець, Ю. А. Чаплинська. 2-е вид, перероб. і доп. Дніпро: Дніпроп. держ. ун-т внутр. справ ; Ліра ЛТД, 2017. 480 с.
11. Цимбал П. В., Кимлик Н. В., Ляшенко М. М. Попередження корупційних злочинів. *Науковий вісник Національного університету державної податкової служби України (економіка, право)*. 2012. № 4. С. 211-216.

Hres I. Cyber crimes of official persons: risks, types and criminalistics measures of prevention

Summary. The article examines specific features of cybercrimes committed by officials. Official crime is a significant threat to society and the normal functioning of the rule of law. This concept unites a significant number of punishable acts provided by the Criminal Code of Ukraine. Official crimes are characterized by a high level of latency and are associated with a violation of citizens' trust in state institutions, undermining the normal functioning of the law enforcement system, and pose a threat to the effective implementation of public administration. The construction of a digital state in Ukraine opens up new opportunities for

the development of society, but at the same time it creates a new field for criminal offenses.

The article analyzes the main risks of committing cybercrimes in the field of professional activity of officials. It was determined that such processes as the digitalization of society in the conditions of the lack of information literacy of public servants, the accumulation of large amounts of information in databases, the low level of legal awareness of officials, the economic crisis, a significant level of corruption in official activities, security flaws and gaps in the protection of database security systems, the discrepancy between the level of knowledge and skills of officials and their salary, as well as the imperfect system of criminal law protection cause an increase in the risks of committing cybercrimes in the field of official activity.

In addition, some types of cybercrimes that can be committed by officials are given, in particular, unauthorized access to information of an intimate nature, abuse of official authority for the purpose of acquiring strategic information or acquiring or using technical resources, manipulating data and documents, abusing technical equipment, destroying or changing evidence

A system of certain means of criminalistics prevention and countermeasures against the commission of cybercrimes by officials is proposed, including: access control, activity monitoring, information protection, creation of a security policy, security and user audits, backup of data and the history of their changes, warning of criminal liability.

Key words: crimes in the field of official activity, official person, pre-trial investigation, corruption crimes, law enforcement officers, cybercrimes, cyber security, criminalistics method of crime investigation, criminalistics prevention, criminalistics prevention and combating of crime.