

1. Статистика кіберзлочинності в Україні [Електронний ресурс]. – Режим доступу: https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_v
2. Статистика кіберзлочинності в Україні [Електронний ресурс]. – Режим доступу: https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_vb
3. Сергій Демедюк, керівник української кіберполіції [Електронний ресурс]. – Режим доступу: <https://www.ukrinform.ua/rubric-technology/2216404-sergij-demeduk-kerivnik-ukrainskoi-kiberpolicii.html>
4. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс] : Указ Президента України. – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/96/2016>
5. Про прийняття за основу проекту Закону України про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Постанова Верховної Ради України. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/1524-19>

Принципи застосування інформаційних технологій в діяльності органів внутрішніх справ.

Калюжна А.О.

студентка 1 курсу ЮД-746 ДДУВС

Гавриш О.С.

науковий керівник, викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

На сучасному етапі продовжується процес формування, удосконалення інформаційних технологій та принципів застосування в діяльності органів внутрішніх справ. Для забезпечення успішного вирішення основних завдань Національної поліції України потребує удосконалення правоохоронної діяльності шляхом оптимізації взаємовідносин з іншими суб'єктами життєдіяльності, зокрема, шляхом інформаційної взаємодії. Це обумовлює необхідність дослідження принципів застосування інформаційних технологій, а також удосконалення форм правового регулювання із забезпечення її

реалізації в діяльності поліції та органами публічної влади і громадськістю.

Завдяки, Ст. 25 закону України «Про Національну поліцію», яка називається «Повноваження поліції у сфері інформаційно-аналітичного забезпечення», в ч.2, яка визначає повноваження поліції в рамках інформаційно-аналітичної діяльності, зазначено, що поліція здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями (п. 4) та вивчає принципи взаємодії.[1] Але слід врахувати недостатній ступінь їх дослідження і вивченості. Бо досягнення соціальних цілей за допомогою закономірностей побудови знаходиться /в даний час, на стадії теоретичного осмислення і супроводжується недостатніми інтересами науково-практичних досліджень.

Закономірності інформаційно-технологічного забезпечення діяльності ОВС об'єктивно впливають з групи закономірностей соціального управління, пов'язаних з реалізацією організаційно-технологічних цілей управління. До групи об'єктивних закономірностей інформаційно-технологічного забезпечення в сфері правоохоронної діяльності відносять:

1. Організації інформаційних технологій управління в сфері правоохоронної діяльності обумовленні особливостями об'єкта інформаційного забезпечення. Ця закономірність непрямо впливає із закону необхідної різноманітності. В агрегованому вигляді об'єктом інформаційного забезпечення є система управління ОВС. При більш детальному, предметному розгляді кола об'єктів інформаційного забезпечення виявляється, що їх перелік на 1-2 порядки перевищує відповідний перелік об'єктів управління. Це пов'язано з тим, що зміст інформаційного забезпечення може ставитися до всього процесу управління, до певних його функцій і стадій, методам і формам, до діяльності окремих управлінських ланок, до конкретних видів керованої правоохоронної діяльності, до діяльності конкретних категорій особового складу та окремих співробітників ОВС і військовослужбовців ВВ. І в кожному з цих випадків забезпечують інформаційні технології будуть характеризуватися своєю специфікою та особливостями. Так, інформаційно-технологічне забезпечення загально-управлінських функцій системи ОВС диференціюється на інформаційні технології прогнозування, планування, організації, регулювання і контролю.[2]

2. Безперервність і циклічність інформаційно-технологічного забезпечення процесу управління в сфері правоохоронної діяльності. Ця

об'єктивна закономірність тісно пов'язана з достатньо вивченою закономірністю циклічності, безперервності процесу управління. Інформаційні технології управління ОВС покликані забезпечувати ряд постійно повторюваних взаємопов'язаних операцій зі збирання, зберігання, обробки, передачі та подання інформації, що забезпечує нерозривність управлінських процедур в часі, циклічний перехід від однієї управлінської функції до іншої.

3. Функціональна спеціалізація інформаційних технологій управління ОВС, яка відбувається в міру ускладнення сфери правоохоронної діяльності. Ця закономірність пов'язана з динамікою соціального розвитку та з особливостями прогресу комп'ютерної індустрії. Традиційні загальноприйняті схеми інформаційного забезпечення сфери правопорядку в умовах реформує суспільство все частіше виявляються неефективними і трансформуються в спеціалізовані підсистеми і комплекси. Розуміння цієї закономірності дасть змогу успішно вирішувати питання співвідношення централізації і децентралізації інформаційно-технологічного забезпечення ОВС, створення і функціонування інформаційних технологій, орієнтованих на функціональну специфіку рішення неоднозначних управлінських завдань в різних регіонах країни.[3]

4. Технологічний консерватизм інформаційного забезпечення правоохоронної діяльності в порівнянні з динамічністю і мінливістю процесів управління. Відповідно до практики діяльності ОВС останніх п'яти-семи років, існуючі структури інформаційно-технологічного забезпечення неминуче застарівають, при цьому швидкість старіння характеризується постійним наростанням. Очевидно, що технологічні перетворення повинні бути адаптивні та з кожним роком все більш досконалішими.

Отже, в даному вигляді загально-управлінської принцип об'єктної орієнтації інформаційних технологій тісно пов'язаний з усіма перерахованими вище загально-управлінської принципами побудови і функціонування систем управління та з принципами здійснення процесу управління системи. І для подальшого використання та розвитку необхідно удосконалення, систематичне вивчення інформаційних технологій, різноманітність висококваліфікованих фахівців, які б допомогли в вдосконаленні, застосуванні та виведенні інформаційних технологій в діяльності органів внутрішніх справ на належний високий рівень.

1. Інформація взаємодія поліції з органами внутрішньої влади [Електронний ресурс] – Режим доступу: <https://yandex.fr/clck/jsredirect?bu=uniq15107351086001934151&from=yandex.fr%3Bsearch%2F%3Bweb%3B%3B&text=>

2. Інформаційні системи органів внутрішніх справ [Електронний ресурс] – Режим доступу: http://stud.com.ua/34590/informatika/informatsiyni_sistemi_organiv_vnutrishnih_sprav

3. Функціональна спеціалізація інформаційних технологій управління ОВС [Електронний ресурс] – Режим доступу: http://stud.com.ua/34592/informatika/informatsiyna_infrastruktura_organiv_vnutrishnih_sprav

4. Система інформаційного забезпечення органів внутрішніх справ (ОВС) України [Електронний ресурс] – Режим доступу: <https://studfiles.net/preview/5536057/page:2/>

Особливості здійснення рейдерства в Україні

Козій В.С.

студент 1 курсу спеціальність «Менеджмент», ДДУВС

Соломіна Г.В.

*науковий керівник, к.е.н., доцент
кафедри економічної та інформаційної безпеки, ДДУВС*

За оцінками експертів, в Україні діє від 35 до 50 професіональних рейдерських груп. Особливість діяльності яких, полягає у захопленні і перерозподілі власності за рамками закону та передбачає використання психологічного тиску, шантажу, підробці документів, підкупі силових структур. Під рейдерські атаки за 2017 рік в Україні вже потрапили 3,7 тисяч суб'єктів господарювання. Річний обсяг перерозподілу сягає від 2 до 3 млрд. доларів США.

Рейдери – це команда висококваліфікованих спеціалістів із захоплення фірми або із перехоплення управління за допомогою навмисне розіграного бізнес-конфлікту. Основна мета рейдерства – приборкання великого бізнесу, великих фірм, підприємств, захоплення значних площ, земельних ділянок, обладнання і нерухомості [1].

Науковці та практики поділяють рейдерів на білих та чорних. Білі рейдери діють методом корпоративного шантажу в рамках чинного