правилам безпеки в мережі Інтернет [3].

Сьогодні, в оборонній сфері, інформаційні ресурси та інформаційна структура оборонного потенціалу країни, яка включає в себе збройні сили та військово-промисловий комплекс, є одними з найважливіших об'єктів безпеки. Сучасні засоби озброєння, військова техніка, системи управління військами та зброєю, є системами критичних додатків з високим рівнем комп'ютеризації, що робить їх дуже вразливими до впливу інформаційної зброї, як у військовий, так і у мирний час.

Ці системи можуть стати предметом атак з використанням програмних закладок, що може призвести до повного або часткового блокування зброї стримування країни до моменту загрозливої ситуації. Така загроза стає дедалі більш актуальною з кожним роком, як свідчить досвід локальних воєн останніх років. Тому, забезпечення безпеки інформаційних ресурсів та структури оборонного потенціалу стає надзвичайно важливим завданням в оборонній сфері [4, 5].

Отже, стратегії захисту є важливим інструментом у забезпеченні національної безпеки від кіберзагроз. Вони мають включати технічні, організаційні та правові заходи, спрямовані на захист інформаційних систем та даних, розробку політики безпеки інформації, підвищення рівня свідомості та навичок громадян з питань безпеки в Інтернеті, співпрацю з іншими державами та міжнародними організаціями в області кібербезпеки, а також захист критичних інфраструктур від кібератак. Забезпечення інформаційної безпеки є невід'ємною складовою національної безпеки, і від цього залежить не тільки ефективне функціонування держави, а й безпека громадян та їхніх прав і свобод.

1. Бєлай С. В., Корнієнко Д. М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. Актуальні проблеми управління інформаційною безпекою держави. Київ: Національна академія Служби безпеки України, 2018. С. 408.

2. Войціховський А. В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. Журнал східноєвропейського права. 2018. № 53. С. 26-37.

3. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 2. С. 16-22.

4. Дмитренко М.А. Проблемні питання інформаційної безпеки України. Міжнародні відносини. Серія Політичні науки. 2017. № 17. С. 236-243.

5. Залєвська І. І., Удренас Г. І. Інформаційна безпека в Україні в умовах російської військової агресії. Південноукраїнський правничий часопис. № 1. 2022. С. 20-26.

УДК 351.74
DOI: 10.31733/17-03-2023-574-575

Олексій ДІДЕНКО
курсант факультету № 4
Харківського національного
університету внутрішніх справ

ЗАСОБИ ВДОСКОНАЛЕННЯ ДІЯЛЬНОСТІ ПОЛІЦІЇ ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Інформаційне суспільство мета більшості сучасних країн світ. В першу чергу, це обумовлено стратегічною перевагою. Такі країни як США, Канада, Японія, члени європейського союзу, вже давно впроваджують інформаційні технології в повсякденні сфери життя.

В основному пов'язаний подальший розвиток інформаційних технологій, з появою нових технічних засобів обробки інформації, які визначають рівень розвитку інформаційних технологій. Покращення управління є найважливішим чинником підвищення ефективності. На основі досягнень ведеться робота з удосконаленням форм і методів управління науково-технічного прогресу, вивчення законів, способів накопичення, обробка та передача інформації.

Згідно з рейтингом міжнародного конкурсу World Digital Competitiveness Ranking [1], Україна у 2021 році посіла 54 місце. Порівняно з 2020 роком показник покращився на чотири позиції. Підсумкова рейтингова система розраховується на основі трьох показників:

якість освіти та науки; регуляторне середовище, фінансовий капітал у ІТ-галузі, стан інтернету та комунікаційних технологій; рівень готовності використання цифрової трансформації. На сьогоднішній день наша держава прагне розпочати новий етап формування інформаційного суспільства. Відбувається перехід від впровадження інформаційних технологій до комплексної побудови цифрової системи в масштабі країни.

Ефективність правоохоронної діяльності значною мірою залежить від якості інформаційного забезпечення, тому інформаційні технології широко використовуються в діяльності правоохоронних органів. Найдоступнішим та найпростішим джерелом інформаційних технологій є сучасний смартфон. Фактично кожен поліцейський може лише за допомогою цього девайса бути на зв'язку з колегами, отримати доступ до онлайн-карт, усіх типів баз даних, навіть дізнатись особисті данні злочинця.

В свою чергу такий легкий доступ до мережі, надає можливість злочинцям порушувати закон, не виходячи з дому. Одним з найпопулярніших видів злочину за допомогою мобільних пристроїв є "онлайн-магазини наркотичних речовин". Більшість з яких працюють через анонімний месенджер "telegram". Такий спосіб збуту має певні переваги: продаж відбувається повністю анонімно, продавець та покупець не мають фізичного контакту [2].

Найпростішим способом боротьби з цим "феноменом" є сам месенджер , в якому є можливість поскаржитись на аккаунт чи канал, набираючи певну кількість скарг, вони блокуються. Існує телеграм бот "стоп наркотик" розроблений працівниками органів внутрішніх справ, який збирає такі канали та дає можливість кожному охочому поскаржитись маючи з собою лише мобільний пристрій, що значно спрощує цю процедуру. Завдяки цьому боту кожен день блокуються сотні аккаунтів.

Ще одним видом використання злочинцями мобільних пристроїв є телефонне шахрайство. Злочинець телефонує жертві представившись працівником банку чи інших установ, та починає запитувати персональні данні. Для запобігання подобних випадків слід дотримуватись наступних рекомендацій: встановити додаток для ідентифікації невідомих номерів, не залишати особисті данні на невідомих сайтах, надавати інформацію про шахраїв відповідним органам.

Висновки. Суспільство широко використовує новітні технології в повсякденному житті, найчастіше, мобільні пристрої. Це стало появою відповідного шахрайства. Органи внутрішніх справ в свою чергу активно використовують мобільні пристрої для протидії відповідній злочинності. Сучасні проблеми потребують сучасного рішення з допомогою засобів захисту інформації та обмеження доступу до персональних даних громадян.

1. World Digital Competitiveness Rankings - IMD. IMD business school. URL: https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/ (дата звернення: 03.03.2023).

2. Пядишев В. Г., Монастирський М. В. Смартфони в руках населення як засіб удосконалення діяльності поліції: порівняння українського та зарубіжного досвіду. Південноукраїнський правничий часопис. 2022, 1-2'. С. 152 158.

УДК 342.95
DOI: 10.31733/17-03-2023-575-578

Олександр ДУНЯШЕНКО
курсант ННІ права та підготовки
фахівців для підрозділів Національної поліції

Науковий керівник:
д.філос.наук, проф. **Елеонора СКИБА**

(Дніпропетровський державний університет внутрішніх справ)

ІНФОРМАЦІЙНА БЕЗПЕКА – ЕЛЕМЕНТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Варто зазначити, що проблема національної безпеки України є особливо актуальною як сьогодні, так і в контексті подальшого загально цивілізаційного розвитку країни. Бурхливий розвиток інформаційної сфери супроводжується появою принципово