Абзалов Денис Владиславович

курсант навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, рядовий поліції

Габорець Ольга Андріївна

доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, доктор філософії, доцент

ЦИФРОВІ ЗАГРОЗИ В УМОВАХ ВІЙНИ: РОЛЬ АНАЛІТИЧНИХ ТЕХНОЛОГІЙ У ЇХ НЕЙТРАЛІЗАЦІЇ

Цифровізація сучасних воєн докорінно змінила природу збройних конфліктів, перетворивши кіберпростір, інформаційні канали та мережеві системи на ключові поля протистояння. У контексті російсько-української війни цифрові загрози набули безпрецедентної масштабності та комплексності, поєднуючи кібератаки, інформаційно-психологічні операції, маніпулятивні медіакампанії, використання штучного інтелекту та високотехнологічних автоматизованих платформ. Критичні інфраструктури – енергетика, зв'язок, логістика, державні реєстри – стають мішенями системних атак, спрямованих на дестабілізацію управлінських процесів, дезорганізацію оборони й підрив суспільної довіри. Паралельно здійснюються багаторівневі інформаційні операції, що використовують ботоферми, фейкові наративи, deepfake-контент і таргетовані маніпуляції з метою впливу на громадську думку, політичну волю та міжнародну підтримку України.

Розвиток бойових дій також супроводжується швидким упровадженням автономних систем і безпілотних платформ, які збирають колосальні масиви даних і, водночас, створюють нові цифрові вразливості. Системи керування дронами, канали передавання телеметрії, алгоритми навігації стають об'єктами атак, спрямованих на підміну даних, перехоплення управління, зниження ефективності розвідки та

вогневої підтримки. Таким чином цифрові загрози перетворюються на багатовимірний феномен, що включає технічні, інформаційні та психологічні чинники, які діють одночасно й синергетично. У цій ситуації традиційні інструменти кіберзахисту виявляються недостатніми, оскільки масштаб і динаміка атак вимагають глибшої аналітики, швидкого перехоплення сигналів, прогнозування тенденцій та прийняття рішень у реальному часі.

На цьому тлі особливої ваги набувають аналітичні технології – OSINT, системи великих даних, інструменти машинного навчання та штучного інтелекту, а також платформи кіберзагрозової розвідки. Саме OSINT забезпечує проактивне виявлення підготовки до кібератак, моніторинг діяльності хактивістських і державних кібергруп, аналіз інформаційних потоків і моделювання взаємозв'язків між цифровими об'єктами [1]. Великі дані, накопичені в умовах війни (фронтове відео, сенсорні потоки, логи атаки, комунікаційні метадані), стають фундаментом для формування ситуаційної обізнаності та підтримки стратегічних рішень. Штучний інтелект дозволяє автоматизувати виявлення аномалій, класифікувати наративи дезінформаційних кампаній, оцінювати ризики та прогнозувати поведінку ворожих кіберструктур.

Водночас противник також вдосконалює свої методи, застосовуючи шифрування, анонімізацію, атаки на моделі машинного навчання, ін'єкції «отруєних» даних і гібридні операції, у яких технічні й психологічні інструменти взаємодіють. Саме тому роль аналітичних технологій доповнюється критично важливим людським чинником: здатністю експертів інтерпретувати дані, перевіряти джерела, оцінювати достовірність інформації та приймати етичні й стратегічно виважені рішення. Не менш значущими залишаються міжнародна співпраця, стандарти кіберстійкості, обмін даними та розвиток власних суверенних технологій штучного інтелекту, інтегрованих у національну систему оборони.

У розвитку цифрового протистояння чітко простежується тенденція до переходу від реактивної до прогностичної моделі безпеки. Аналітичні технології дозволяють не лише фіксувати інциденти, а й визначати закономірності їх розвитку, виявляти «слабкі сигнали» майбутніх атак,

прогнозувати цілі противника й будувати сценарії реагування. Війна дедалі більше перетворюється на змагання швидкості обробки даних, точності аналітичних моделей і здатності приймати рішення на основі комплексних інформаційних масивів. Держава, що ефективно інтегрує ці технології, отримує перевагу в інформаційному, кібернетичному та оперативному доменах, а відтак – у загальній системі оборони.

Цифрові загрози в умовах війни становлять складну, багатокомпонентну систему, що охоплює технічні, інформаційні та психологічні впливи. Їх нейтралізація неможлива без аналітичних технологій, які забезпечують перетворення масивів даних на операційно значущі знання, підтримують раннє виявлення атак, прогнозування ризиків та ефективну координацію оборонних дій. Успішна протидія цифровим загрозам вимагає синергії технологічних інновацій, якісної кіберзагрозової розвідки, інституційної та міжнародної співпраці, а також людиноцентричного підходу. Саме ця інтегрована модель забезпечує державі стійкість та адаптивність у гібридній війні XXI століття.

Література

1. Габорець О. А. Використання OSINT-технологій при розкритті шахрайств, учинених в кіберпросторі : робота на здобуття кваліфікаційного ступеня магістра: спец. 125 - Кібербезпека та захист інформації / наук. кер. В. В. Муж. Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2024. 80 с.