УДК 343.9:004.738.5(075.8)

Володимир Михайлович Струков,
кандидат технічних наук, доцент, професор кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Дмитро Юрійович Узлов,
кандидат технічних наук, начальник управління інформаційно-аналітичної підтримки ГУНП в Харківській області

Аділь Рза Огли Пірієв,
генеральний директор компанії «Vega-Plus» (Азербайджан, Баку)

Сучасні високотехнологічні тренди у кримінальному світі

Процес стрімкого переходу більшої частини відносин матеріального світу в віртуальну сферу супроводжується бурхливим розвитком як легальної складової ІТ-сфери так і нелегальної. Причому спостерігається певна паралельність (дзеркальність) цих процесів. Відмітимо дві характерні особливості. Перша полягає в тому, що стрімко зростає число доступних через Мережу «некваліфікованих користувачів», в першу чергу, внаслідок всеосяжного поширення смартфонів. По-друге, стрімко розвивається і розгалужується високотехнологічна і високопрофесійна частина ІТ-сфери. Причому рівень і темпи розвитку нелегальної частини цього напрямку не відстає від легальної. Є дані, що вже в даний час всередині корпоративних мереж лідерів американського хайтека і біотехнологій діють багатоцільові і багатофункціональні хакерські програмні модулі, побудовані на основі самовдосконалючихся програм.

Правоохоронці по всьому світу всерйоз готуються до появи підпільних синдикатів, що спеціалізуються на замовних високотехнологічних вбивствах і терактах, замаскованих під технічні інциденти різного роду. Беручи до уваги обсяг ринку замовних вбивств в Сполучених Штатах, що становить близько 2 млрд дол. на рік, а також зростаючу активність терористичних угруповань, очікується поява таких мережних синдикатів протягом найближчих двох років.

У 2014 р. в Мексиці в одному з віддалених районів столиці країни завдяки успішним діям агентурної розвідки був розкритий завод по збірці дронів різних конструкцій, що належить одному з наркосиндикатів. Цей завод виробляв транспортні дрони і готувався налагодити виробництво бойових дронів прикриття. Ці дрони повинні супроводжувати транспортні дрони і виводити з ладу поліцейські автомобілі, оснащені радарами повітряного спостереження[1].

За інформацією російських спецслужб в штабі ІГІЛ створено підрозділ високотехнологічних терактів. Бойовики роблять ставку на малі керовані літальні системи: дрони з саморобними бомбами, які планується використовувати для терактів в країнах Європи.

Зараз ринок високотехнологічних інструментів насичений сучасними ефективними рішеннями, причому вартість компонентів, що включають елементи складних інтелектуальних і конструктивних рішень, стрімко здешевлюється, що робить їх доступними не тільки великим потужним структурам, а й невеликим групам і навіть окремим фізичним особам. Так, наприклад, на сайті китайської кампанії ali baba вічко для дверей, яке укомплектоване наукоємною технологією 3D-розпізнавання обличчя, коштує лише 120 дол. США.

В результаті стрімкого розвитку біотехнологій та генної інженерії останні роки склалася парадоксальна ситуація: «за оцінками експертів, лабораторія з виробництва біологічної зброї в сучасних умовах разом з усім обладнанням може коштувати в межах від декількох десятків до декількох сотень тисяч доларів США, а в якості біологічної зброї можуть бути використані і ті патогени, які конвенціонально не заборонені для застосування в дослідницьких цілях, отримання діагностичний систем, вакцин та інших медичних препаратів. Найбільш значущими загрозами біотероризму є різке збільшення числа фахівців з біотехнологій, доступність інформації за рецептурами біологічних та бактеріологічних препаратів, а також можливість легендування окремих актів біотероризму під прояви природних епідемій і інфекцій.

В кінці 2005 р. генетик Р. Брент з Каліфорнійського інституту молекулярних наук (Molecular Sciences Institute – MSI) провів експеримент, який доводить, що сьогодні технології в генній інженерії досягли вже такого рівня, коли один тлумачний лаборант з невеликим обсягом «правильних» ресурсів може виготовити біологічну зброю зі згубною міццю, яка не поступається атомній бомбі.

Американський вчений Р. Карлсон, фізик і біолог, який працював деякий час з Брентом в MSI, прогнозує, що приблизно протягом наступного десятиліття створення біологічної зброї з нуля стане настільки ж легким і дешевим, як побудова сайту.»[1].

Яскравою ілюстрацією такого становища є наступний випадок[1].

«У червні 2006 року співробітники британської газети The Guardian з'ясували, що створити біологічну зброю сьогодні може буквально будь-який зацікавлений в цьому житель Сполученого Королівства. Увагу журналістів привернув сайт компанії VN Bio Ltd, яка здійснювала постачання обладнання та витратні матеріали для біологічних лабораторій. В одному з каталогів біосировини були знайдені вельми дивні «товари» – на продаж виставили фрагменти ДНК смертельно небезпечних для людини вірусів віспи та іспанського грипу. Для оформлення замовлення на ДНК віспи знадобилося лише надати адресу, номер мобільного телефону та адресу електронної почти – вже через три години до редакції The Guardian подзвонив кур'єр і повідомив, що замовлення доставлено. Ніяких перевірок того, кому відправляється потенційно небезпечний вантаж, проведено не було – отримувачем міг би виявитися як законослухняний вчений, так і можливий терорист».

«Справжнім кошмаром для розвідувальних і правоохоронних структур усіх країн світу є бойові роботи, оснащені біологічною і хімічною зброєю. Щоб створити бойового робота, який використовує біологічну зброю, досить використати розроблені в даний час дрони сільськогосподарського призначення, заповнивши відповідні їх ємності не добривами, а бактеріями, вірусами або хімічними сполуками. Вартість сільськогосподарського дрона з дальністю польоту до 150 км і ємністю завантаження до 50 л становить лише 6 тис. дол. США, а ємністю до 200 л – менше 9 тис. дол. Купівля такого дрона доступна не тільки терористичній мережі, а й окремій групі фанатиків і екстремістів. «

Якщо брати до уваги наступні очевидні факти: 1) деякі терористичні організації (ТО) та організовані злочинні групи (ОЗГ) мають бюджет, більший ніж в деяких країнах; і 2) керівники ТО та ОЗГ є люди, як правило, не обділені розумом, і дуже прагматичні, а також деякі події останніх років, то можна дійти до простого логічного висновку – якщо правоохоронні структури будь-якої держави будуть «пасти задніх» у технологічних рішеннях, то безпека громадян, бізнесу і держави в цілому в цих країнах буде знаходитися під великою загрозою.

Так, наприклад, навіть керівники ФБР вважають, зокрема, що Америка сьогодні не готова до відсічі хакерським угрупованням, що націлені на інтелектуальну власність, що належить корпораціям, федеральному уряду і університетам [1].

Список бібліографічних посилань

1. Овчинский В. С. Криминология цифрового мира : учеб. М. : Норма ; Инфра-М, 2018. 352 с.
2. Gartner: Топ-10 стратегических трендов развития технологий в 2019 году // Київський міжнародний економічний форум : сайт. 26.10.2018. URL: https://ain.ua/2018/10/26/gartner-top-10-trendov-razvitiya-texnologij/ (дата звернення: 27.10.2019).

Одержано 29.10.2019