Таким чином, переміщення повітряних суден, що здійснюється в повітряному просторі, вимагає впорядкування, визначення спеціального режиму використання повітряного простору та управління з боку держави, яке здійснюється Державною авіаційною службою.

Література

1. Шульженко Ф. П. Транспортне право: навч. посіб. / Ф. П. Шульженко, О. А. Гайдулін, Р. С. Кундрик. – К.: КНЕУ, 2005. – 244 с.
2. Стеценко С. Г. Адміністративне право України: навч. посіб. / С. Г. Стеценко. – К.: Атіка, 2007. – 624 с.
3. Про транспорт: Закон України від 10 листопада 1994 р. № 232/94-ВР // Відомості Верховної Ради України. – 1994. – № 51. – Ст. 446.
4. Повітряний кодекс України від 19 травня 2011 р. № 3393-VI // Відомості Верховної Ради України. – 2011. – № 48-49. – Ст. 536.

УДК 341:656.7.01

Степанцова Ю. Ю., студентка,
Навчально-науковий Гуманітарний інститут,
Національний авіаційний університет, м. Київ
Науковий керівник: Радзівілл О. А., к.ю.н., доцент

ЗАПОБІГАННЯ НЕЗАКОННОГО ВТРУЧАННЯ В ДІЯЛЬНІСТЬ АВІАЦІЙНИХ КОМУНІКАЦІЙ

У сучасних реаліях комп’ютеризація пронизує майже всі сторони суспільного життя – від контролю за повітряним і наземним транспортом до вирішення проблем національної безпеки. Проте, швидкий інформаційний розвиток суспільства поряд із позитивними досягненнями, супроводжується й низкою негативних явищ. Особливо це стосується збільшення кількості злочинів у сфері комп’ютерних систем та мереж, оскільки такі злочини не лише гальмують позитивні тенденції розвитку, а й завдають шкоди суспільству та державі.

Не оминула ця проблема й системи обслуговування діяльності цивільної авіації. Новітні досягнення в області інформаційних технологій та засобів комунікації, сприяли не тільки розвитку авіації, але і створили основу для нового виду злочину, так званого кібертероризму.

Відносна новизна цього злочину, застали зненацька правоохоронні органи, які виявилися не готовими до адекватного протистояння й боротьби з новим соціально-правовим явищем [1].

Спектр проявів авіаційного кібертероризму досить широкий – від незаконного впливу на системи контролю вильоту та на

інформаційні бази льотних завданьдо злому диспетчерських системта проникнення в системи бронювання й реєстрації пасажирів.

З такими проявами поки що досить складно вести ефективну боротьбу як з точки зору кримінального переслідування, так і в царині упереджу вальних заходів. Це пов'язано з тим, що у кібертероризму відсутні будь-які державні кордони, наявне відмінне матеріально-технічне оснащення, жорстка конспірація тощо [2].

Отже цілком закономірно, що боротьба зі злочинами у сфері комп'ютерної інформації із внутрішньодержавного переходить у міжнародне правове середовище. Світова практика боротьби з правопорушеннями, пов'язаними із застосуванням комп'ютерної техніки, доводить необхідність міждержавної співпраці у боротьбі з останніми [3]. На жаль, головною зброєю у боротьбі з кібертероризмом на сьогодні залишаються різні міжнародні та національні нормативні та правові акти у даній галузі.

Найбільш значною у сфері розробки кримінально-правових і процесуальних аспектів боротьби із даною категорією злочинів є діяльність Організації Об'єднаних Націй, Організації економічного співробітництва і розвитку, Європейського Союзу, Ради Європи, Інтерполу та деяких інших.

Одними з основнихміжнародно-правових документів у питанні правового регулювання міжнародних відносин у сфері кібербезпеки є Конвенція ООН проти транснаціональної організованої злочинності, Віденська декларація про злочинність і правосуддя: відповіді на виклики XXI століття (ООН), Європейська Конвенція про кіберзлочинність тощо.

Що стосується саме галузі авіації, то основним документом, що регулює питання боротьби з кіберзлочинністю, є Міжнародна конвенція про кіберзлочинність від 23 листопада 2001 року. Цей документ націлений на здійснення загальної політики з питань кримінального права, метою якої є захист суспільства від кібертероризму шляхом прийняття потрібних законодавчих актів, а також шляхом розширення міжнародного співробітництва.

Щодо інших запобіжних заходів світової спільноти можна зазначити: створення національних стратегій безпеки від кібертероризму; створення військових підрозділів для боротьби з кібератаками; відкриття Європейського центру по боротьбі з кіберзлочинністю, який фактично став координаційним центром ЄС у боротьбі із кіберзлочинністю тощо.

Отже, можна зробити висновок, що за сучасних умов прояв кібертероризму в авіаційній галузі з кожним роком буде зростати. Відповідно сучасні проблеми забезпечення кібернетичної безпеки авіаційної галузі будуть пов'язані з розв'язанням найближчим часом

низки потреб різного характеру. Для цього, перш за все, необхідно: посилити регулювання на національному та міжнародному рівнях діяльності в кіберпросторі (шляхом укладання угод стосовно використання кіберпростору, а також охорони авіаційної комунікації від кібератак); удосконалити вітчизняне нормативно-правове забезпечення; збільшити фінансування сектору кібербезпеки; приділити увагу покращенню фахової підготовки спеціалістів в області кібербезпеки та розширити її орієнтуючись на потреби цивільної авіації.

Література

1. Голубєв В. А. Кібертероризм – міф чи реальність? [Електронний ресурс] / В. А. Голубєв. – Режим доступу: http://www.crime-research.org/library/terror3.htm

2. Харченко В. П. Кибертерроризм на авиационном транспорте / В. П. Харченко, Ю. Б. Чеботаренко, О. Г. Корченко, Е. В. Пацира, С. О. Гнатюк // Проблеми інформатизації та управління: зб. наук. пр.: Вип. 4 (28). – К.: НАУ, 2009. – С. 131-1405.

3. Сеитов Т. Б. Международно-правовое сотрудничество государств в борьбе с компьютерной преступностью: автореф. дис. … канд. юрид. наук: 12.00.10 / Т. Б. Сеитов – Алматы, 2002. – 25 с.

УДК 341:656.7.01(043.2)

Шморгун М. С., студентка,
Навчально-науковий Гуманітарний інститут,
Данченко Т. С., студентка,
Навчально-науковий Юридичний інститут,
Національний авіаційний університет, м. Київ
Науковий керівник: Радзівілл О. А., к.ю.н., доцент

СУТЬ ТА ВИДИ КІБЕРЗЛОЧИНІВ

Кіберзлочини – це злочини у «віртуальному просторі» – змодельованого за допомогою комп’ютера інформаційному просторі, в якому знаходяться відомості про осіб, предмети, факти, події, явища і процеси, представлені в цифровому, символьному або будь-якому іншому вигляді. Будапештська Конвенція Ради Європи про кіберзлочинність від 23.11.2001 р. (далі – Конвенція) поділяє кіберзлочини на такі категорії: 1) правопорушення проти конфіденційності, цілісності та доступності комп’ютерних даних і систем (так звані «CIA-злочини»); 2) правопорушення, пов’язані з комп’ютерами, включаючи підробку і шахрайство, здійснені з використанням комп’ютерів; 3) правопорушення, пов’язані зі змістом інформації, зокрема, дитяча порнографія, расизм та ксенофобія;