М. И. Борис
Научный руководитель — кандидат юридических наук А. А. Шафалович
БГЭУ (Минск)

КИБЕРПРЕСТУПНОСТЬ. ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ

Сегодня практически каждый шаг современного человека связан с информационными технологиями, которые предоставили стимул для прогресса общества, но и спровоцировали появление и формирование «компьютерных правонарушений» — киберпреступности. Следует отметить, что общепринятого определения до настоящего времени нет. К киберпреступлениям можно отнести любое преступление, совершенное в электронной среде с использованием компьютера.

По официальной статистике в Республике Беларусь отмечается значительный рост количества преступлений, связанных с компьютерной техникой и информационными технологиями. По итогам 10 месяцев 2019 г. количество киберпреступлений в Беларуси выросло в 2,2 раза (с 3518 до 7694) в сравнении с аналогичным прошлогодним периодом. Особенность таких преступлений заключается в их высокой латентности (более 85 %) и появлении новых способов их совершения [1].

Компьютерные правонарушения совершаются по различным мотивам и разными лицами (как специалистами в сфере информационных технологий, так и обычными пользователями).

Среди проблем противодействия таким преступлениям — сложность доказательства вины правонарушителя, отыскания улик, установления свидетелей, а также своевременного пополнения багажа знаний сотрудников правоохранительных органов в этой специфической сфере. Кроме того, многие юридические лица предпочитают решать возникающие проблемы без участия правоохранительных органов, опасаясь, что убытки от расследования киберпреступления могут оказаться выше суммы причиненного ущерба. Поскольку правоохранительные органы, как правило, изымают на срок до двух месяцев сервер для производства судебной экспертизы, что может привести к проблемам в деятельности юридического лица. Руководство пострадавшей организации опасается подрыва репутации и (или) выявления в процессе расследования различных правонарушений в работе компании [2].

В настоящее время возникает необходимость разработки и совершенствования мер противодействия киберпреступлениям (технических, организационных и правовых). Среди них — разработка и реализация специальных программных и аппаратных комплексов безопасности, резервирование систем, подбор персонала, разработка норм, устанавливающих ответственность за ком-

пьютерные правонарушения, защита авторских прав программистов, устранение правовых пробелов в законодательстве, установление правил лицензирования и сертификации в области защиты информации. Необходимо повышать доверие между правоохранительными органами и организациями всех форм собственности, объединять их усилия в предупреждении, выявлении, пресечении и расследовании киберпреступлений. Учитывая, что компьютерная преступность — это проблема международного масштаба, необходимо расширять сотрудничество на региональном и международном уровне.

И с т о ч н и к и

1. В Беларуси прогнозируют рост киберпреступности в 2020 году [Электронный ресурс] // Naviny.by. Белорусские новости. — Режим доступа: https://naviny.by/new/20191127/1574876254-v-belarusi-prognoziruyut-rost-kiberprestupnosti-v-2020-godu. — Дата доступа: 22.02.2020.

2. *Косович, М. В.* Компьютерная преступность: уголовно-правовые и криминологические вопросы (часть 2) [Электронный ресурс] : [по состоянию на 03.06.2019 г.] / М. В. Косович, Н. И. Лимож // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. — Минск, 2020.