

# ВВЕДЕНИЕ

С появлением современных средств вычислительной техники и телекоммуникаций традиционные преступления – воровство, мошенничество, шпионаж, вымогательство трансформировались в новые формы. Кроме того, появились специфические для компьютерных систем<sup>1</sup> и сетей преступления. Намечается тенденция к использованию информационных технологий организованными преступными группами и распространение их деятельности на межгосударственный уровень. Сотрудники правоохранительных органов при раскрытии и расследовании компьютерных преступлений неизбежно сталкиваются с большими трудностями, так как преступления в сфере компьютерной обработки информации характеризуются высокой скрытностью, трудностями сбора улик по установлению фактов их совершения, сложностью доказывания в суде. Субъекты преступлений – это, как правило, высококвалифицированные программисты, инженеры, специалисты в области телекоммуникационных систем, банковские работники, бывшие сотрудники спецслужб.

Есть основания утверждать, что при переходе цивилизации к информационному обществу все большее количество преступлений будет совершаться в инфосфере. Мировое сообщество крайне озабочено состоянием защиты национальных информационных ресурсов в связи с расширением доступа к ним через различные открытые информационные сети.

Несмотря на определенное количество исследований и публикаций, проблема раскрытия и расследования компьютерных преступлений, в частности проведения ряда первоначальных следственных действий, изучена явно недостаточно, а проблемным вопросам компьютерного следоведения посвящено чрезвычайно мало работ.

Приступая к написанию данной книги, мы ставили перед собой цель изложить научнообоснованные рекомендации для сотрудников правоохранительных органов Республики Беларусь и Российской Федерации – не специалистов в области вычислительной техники и электроники. Указанные рекомендации могут быть использованы:

---

<sup>1</sup> Здесь и далее под компьютерной системой мы понимаем локальные ЭВМ, персональный компьютер, сервер или рабочую станцию вместе с периферийными устройствами.

- для оптимизации труда следователя при расследовании дел о компьютерных преступлениях, а также преступлениях в финансовой и банковской сфере, преступлений, связанных с электронным шпионажем;
- совершенствования тактики проведения следственных действий при расследовании дел рассматриваемой категории;
- совершенствования использования специальных знаний в процессе раскрытия и расследования указанных дел;
- совершенствования систем информационной безопасности субъектов хозяйствования.

Собранные и систематизированные материалы могут быть использованы в преподавании учебных курсов криминалистики, информатики, информационной безопасности в высших и средних специальных учебных заведениях юридического профиля.

Проблема борьбы с компьютерными преступлениями многоаспектна. Осознавая это, автор счел необходимым в **разделе 1** учебного пособия рассмотреть основы информационной безопасности. Рассматриваемый материал является продуктом широкого обобщения. На данную тему в свое время писали многие ученые ближнего и дальнего зарубежья. Так, правовые аспекты, например, нашли свое отражение в работах В. М. Аверьянова, Н. Ф. Ахраменка, Ю. М. Батурина, А. В. Венгерова, Э. П. Крюковой, Ю. К. Орлова, А. Л. Савенка, А. Б. Тельба, А. Г. Эджубова; общие вопросы комплексной защиты информации – в работах В. В. Анищенко, В. С. Барсукова, В. Гайковича, А. Б. Желкова, В. В. Кульбы, Д. Керра, В. А. Конявского, В. Д. Курушина, А. П. Леонова, В. А. Минаева, А. Першина, А. В. Петракова, С. Мэджика, У. Пэрри, В. К. Фисенко, В. И. Ярочкина и многих других; криминалистические аспекты – в работах Д. Айкова, Б. Е. Богданова, Р. С. Белкина, В. Б. Вехова, А. В. Гортинского, С. П. Голубятникова, А. Н. Караханьяна, В. В. Крылова, Г. Н. Мухина, Н. С. Полевого, К. Сейгера, Н. А. Селиванова, Б. Х. Толеубековой, У. Фонсторха, С. П. Фортинского, В. Н. Черкасова.

**Раздел 2** посвящен криминалистической характеристике компьютерных преступлений. При написании этого и следующего раздела нами широко использовались данные самостоятельно проведенного исследования. Целью публикации раздела является определение понятия, структуры и содержания криминалистической характеристики компьютерных преступлений.

**Раздел 3** посвящен проведению отдельных следственных действий по делам рассматриваемой категории на основании сформулированных теоретических положений криминалистической характеристики. Нами даются

выдача практические рекомендации по использованию технико-криминалистических средств, тактике проведения осмотра места происшествия, тактике назначения и производства экспертиз, в том числе непосредственно на месте происшествия, тактике использования специальных знаний и особенностям выдвижения следственных версий на этапе осмотра места происшествия по делам о компьютерных преступлениях.

Недостаточная разработанность упомянутых выше аспектов, имеющих существенное значение для успешной борьбы с преступностью и развития науки криминалистики, уголовного процесса и информатики, подтолкнуло автора на написание данного учебного пособия.