УДК 343.98

К. Е. Кузьмин
курсант 343 взвода факультета обеспечения безопасности на транспорте
Белгородского юридического института
МВД России имени И. Д. Путилина

Научный руководитель: ***А. М. Журбенко****,*
доцент кафедры криминалистики
Белгородского юридического института МВД России
имени И. Д. Путилина,
кандидат экономических наук

УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ И КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации — это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. С развитием современного мира данное понятие все чаще встречается в нашей жизни. Так, на сегодняшний день с развитием киберпространства Российской Федерации, согласно открытым данным Генеральной прокуратуры России, зафиксирован существенный рост развития киберпреступности [1]. Также из-за роста количества совершаемых преступлений в сфере компьютерной информации, высокой степени их латентности, резкого увеличения наносимого ими ущерба, они ставят разработку методов совершенствования уголовно-процессуальной и криминалистической деятельности правоохранительных органов по предупреждению, выявлению и расследованию рассматриваемых преступлений на первое место. Защищаемая информация может составлять государственную, служебную и иные виды охраняемой законом тайны, каждый из которых имеет свои особенности в области регламентации, организации и осуществления этой защиты. Для того чтобы более подробно разобраться в данном вопросе, необходимо рассмотреть как уголовно-процессуальные, так и криминалистические аспекты защиты такой информации в борьбе с киберпреступностью и дать более подробное определение защиты компьютерной информации.

Защита компьютерной информации — это комплекс мер и технологий, направленных на обеспечение конфиденциальности, целостности и доступности информации, хранящейся и передаваемой через цифровые системы. Она включает в себя различные аспекты, такие как защита от несанкционированного доступа, предотвращение утечек данных, обеспечение безопасности сетей органов

внутренних дел (далее — ОВД) Российской Федерации. Основными аспектами для защиты компьютерной информации в целом являются шифрование данных, аутентификация, авторизация и управление доступом к защищаемой информации [2]. Защита информации в ОВД имеет особое значение, поскольку эти органы работают с конфиденциальными и чувствительными данными, связанными с правопорядком, уголовными расследованиями, личной информацией и другими аспектами правопорядка. В настоящее время защита информации не ограничивается только решением задач сохранения секретных сведений от возможной утечки или утраты. Широкое использование компьютерной техники при обработке, накоплении и хранении информации требует обеспечения защиты информационных массивов от разрушения, искажения, подделки, блокирования и иных вмешательств в информацию и информационные системы ОВД Российской Федерации. Защита информации тесно связана с обеспечением режима секретности, который представляет собой комплекс мер по защите информации на конкретном объекте (в Министерстве внутренних дел, структурных подразделениях) или при выполнении определенной работы. Основная задача режима секретности заключается в установлении на режимном объекте уровня защиты информации, соответствующего степени секретности имеющихся там защищаемых сведений.

Основными задачами защиты информации являются защита государственной тайны, охрана межгосударственных секретов. Помимо этого, к иным, второстепенным задачам в этой области можно отнести:

- обеспечение конфиденциальности информации;
- сохранение ее целостности.

Решение этих задач осуществляется с помощью правовых, организационных, инженерно-технических и программно-математических мер по защите информации [3].

Уголовно-процессуальные аспекты защиты цифровой информации в ОВД включают в себя ряд важных моментов, связанных с предотвращением, расследованием, раскрытием и связанных с использованием информационных технологий. Говоря об уголовно-процессуальных аспектах защиты компьютерной информации, стоит также перечислить основные составляющие, к которым относятся:

- сбор и хранение цифровых доказательств;
- проведение служебных мероприятий в цифровой среде;
- нормативно-правовые акты (включая Уголовный и Уголовно-процессуальный кодексы Российской Федерации).

Если брать во внимание сбор и хранение цифровых доказательств, стоит отметить, что это представляет собой важный аспект в обеспечении эффективного расследования и судебного разбирательства в области

информационно-телекоммуникационных технологий и других преступлений, связанных с использованием информационных систем. Сбор цифровых доказательств должен осуществляться с соблюдением способов и методов, которые гарантируют сохранность и целостность данных. Это может включать изъятие компьютеров, мобильных устройств и других носителей информации, а также фиксацию сетевого трафика и иных цифровых следов [4]. Проведение служебных мероприятий в цифровой среде представляет собой процесс, включающий использование специализированных методов и технологий для сбора, анализа и интерпретации цифровых доказательств в рамках расследования преступлений, связанных с использованием информационных технологий. Что касается одного из самых важных уголовно-процессуальных аспектов в этой области — нормативно-правовых актов, то стоит сказать, что ОВД должны соблюдать законодательство и нормативные акты, касающиеся цифровой информации, включая расследование киберпреступлений, нарушений конфиденциальности данных и других преступлений в сфере информационных технологий.

Криминалистические аспекты защиты цифровой информации в ОВД охватывают широкий спектр деятельности, связанный с обеспечением безопасности, анализом электронных доказательств и борьбой с киберпреступностью. Рассматривая криминалистические аспекты защиты компьютерной информации, стоит отметить, что к главным аспектам можно отнести:

- цифровые доказательства;
- цифровую криминалистику;
- идентификацию цифровых доказательств.

Если более подробно говорить о каждом из этих аспектов, стоит отметить, что к цифровым доказательствам относятся различного рода электронные следы, а также жесткие диски, мобильные устройства, сетевой трафик и т. д. Цифровая криминалистика, в свою очередь, — это специализированная область криминалистики, которая охватывает методы извлечения и анализа цифровых доказательств с целью подтверждения или опровержения киберпреступлений и является одним из аспектов защиты информации. Идентификацией цифровых доказательств занимаются специалисты-криминалисты ОВД. К такой идентификации относится обнаружение, изъятие и анализ цифровых улик, включая компьютеры, мобильные устройства, носители информации и сетевой трафик, с целью выявления электронных следов преступлений.

Подводя итог данной работе, можно сделать вывод о том, что защита компьютерной информации является важным аспектом в современном информационном обществе и требует комплексного подхода, включающего технологические, организационные и человеческие ресурсы для обеспечения безопасности данных.

1. Журбенко А. М., Махмутов А. Р. К вопросу о формировании единого банка цифровых следов интернет-пользователей для раскрытия преступлений // Современное уголовно-процессуальное право — уроки истории и проблемы дальнейшего реформирования : сб. материалов междунар. науч.-практ. конф., посвящ. 100-летию принятия УПК РСФСР 1922 г., 20-летию действия УПК РФ, Орел, 6–7 окт. 2022 г. : в 2 ч. Орел : Орлов. юрид. ин-т МВД России им. В. В. Лукьянова, 2022. С. 143–146. Вернуться к статье

2. Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения [Электронный ресурс] : ГОСТ 2.051-2013 : введ. приказом Росстандарта от 22.11.2013 г. № 1628-ст. Доступ из справ.-правовой системы «КонсультантПлюс». Вернуться к статье

3. Зуев С. В. Электронное копирование информации — регламентация в УПК // Законность. 2013. № 8. С. 22–23. Вернуться к статье

4. Савицкая И. Г. Участие специалиста в следственных действиях, связанных с изъятием электронных носителей информации // Судебная власть и уголовный процесс. 2016. № 2. С. 250–254. Вернуться к статье