УДК:

Аракелян А.Г.

Студент 3 курса

Группа: ЮРП-б-о-22-4

Северо-Кавказский федеральный университет

(г. Ставрополь, Россия)

Овчаренко И.А.

К.ю.н, доцент кафедры уголовного права и процесса

Северо-Кавказский федеральный университет

(г. Ставрополь, Россия)

КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация: *Работа посвящена анализу криминалистических аспектов обеспечения информационной безопасности и защиты информации в рамках досудебного производства. Отмечается отсутствие в криминалистике устойчивого определения понятия информационной безопасности, что затрудняет её нормативное и прикладное использование в доказательственной деятельности. Раскрываются теоретические и практические основания для интеграции принципов защиты информации в структуру уголовного преследования. Рассмотрены особенности использования криминалистических средств в целях охраны доказательственных сведений от утраты, искажения и несанкционированного доступа. Подчёркивается значение междисциплинарного подхода при разработке эффективных методик фиксации и хранения цифровых следов. Обосновывается необходимость систематизации понятийного аппарата и выработки единых стандартов, обеспечивающих достоверность и допустимость информации, полученной в процессе расследования.*

Ключевые слова: *криминалистика, информационная безопасность, защита информации, доказательства, криминалистические средства, сохранность данных.*

Понятийная конструкция информационной безопасности в пределах криминалистики на сегодняшний день остаётся неразработанной. Отсутствуют определения, фиксирующие содержание и границы данного явления применительно к различным стадиям уголовного судопроизводства [3].

В целом, информационная безопасность представляет собой комплекс научных знаний и практических механизмов, направленных на предотвращение

несанкционированного доступа, использования, раскрытия, искажения, модификации, исследования, регистрации либо уничтожения сведений независимо от формы их существования. Концепция развивается на стыке кибернетики, юриспруденции и прикладной математики, формируя междисциплинарный каркас, обеспечивающий сохранность доказательного материала при возрастающем цифровом давлении.

Свои определения информационной безопасности сформулировала и наука. Правда, в научной литературе отсутствуют однозначные подходы к определению этого понятия. Часть авторов определяет информационную безопасность на основе, в целом, технического подхода к этому понятию. Так, например, поступают в своей коллективной статье В.Ю. Статьев и В.А. Тиньков. Они пишут, что информационная безопасность есть защита информации и поддерживающей ее инфраструктуры с помощью совокупности программных, аппаратно-программных средств и методов с целью недопущения причинения вреда владельцам этой информации или поддерживающей ее инфраструктуре. Относительно характера защищаемой информации можно сказать, что к ней следует отнести всю доказательственную и ориентирующую информацию, добываемую в процессе досудебного производства. Также это информация, добываемая на основе сопровождения оперативными службами этапов возбуждения уголовного дела и предварительного расследования, ее, дознаватель, следователь и прокурор, на основе принципов криминалистического взаимодействия с оперативными службами, использую в процессе расследования уголовного дела. Защита данной информации осуществляется на протяжении всего периода досудебного производства, а в исключительных случаях и в процессе судебного производства с целью обеспечения нормального слушания уголовного дела [2].

Понятие защиты информации формируется на пересечении теории систем, кибернетики и правовых наук, отражая совокупность организационных и технических мер, препятствующих утечке, искажению и несанкционированному доступу к сведениям. Научное сообщество

рассматривает данную категорию как динамический процесс, адаптирующийся к меняющемуся вектору угроз цифровой эпохи. Системная модель защиты опирается на три взаимодополняющих принципа: сохранение целостности, охрану конфиденциальности и обеспечение доступности; каждый названный элемент выступает обязательным условием надёжной информационной среды. Реализация указанной модели требует строгого контроля привилегий, криптографического укрепления коммуникационных каналов, регулярного аудита, а также непрерывного мониторинга аномалий посредством методов машинного обучения. Комплексность задачи обусловила необходимость разработки междисциплинарных методик, в которых инженерные решения сочетаются с нормативно-правовыми регуляторами и криминалистическими процедурами фиксации цифровых следов [6].

Особое значение в правовом регулировании указанной сферы имеет Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Его положения формируют нормативную основу обращения с информацией и определяют обязательные требования к обеспечению её безопасности, в том числе в процессе уголовного судопроизводства [1].

Система криминалистических средств, направленных на обеспечение информационной безопасности, формируется как совокупность взаимосвязанных методов, процедур и технических решений, включающих приёмы тактического воздействия, алгоритмы оперативного анализа и методические действия, применяемые в рамках уголовного преследования. Анализ досудебной стадии показывает, что применение указанных средств способствует достижению устойчивого процессуального преимущества за счёт обеспечения сохранности доказательственной информации, защиты её от искажения, утраты либо несанкционированного вмешательства [4]. Объединение криминалистического инструментария с задачами защиты информации усиливает функциональные возможности следователя, создавая условия для достоверного установления фактических обстоятельств и

формирования надёжной доказательной базы. Технические компоненты защиты приобретают особое значение в работе с цифровыми носителями, где требуется соблюдение принципов неизменности, верифицируемости и воспроизводимости [5]. Осмысление информационной безопасности как элемента криминалистической деятельности предполагает не только сохранение доступа к данным, но и обеспечение их доказательной пригодности, что требует унификации методик, нормативного закрепления процедур хранения и передачи сведений, а также внедрения критериев оценки цифровых следов. Проблематика интеграции понятий защиты информации в структуру криминалистики подтверждает необходимость выработки методологической базы, способной учесть специфику процессуальных интересов, технологии сбора цифровых улик и требования доказательственного стандарта. Проведённый анализ позволяет утверждать, что обеспечение информационной безопасности в рамках уголовного судопроизводства приобретает неотъемлемое значение для криминалистической теории и практики, так как напрямую влияет на достоверность и допустимость результатов процессуальной деятельности.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ. URL: https://www.consultant.ru (дата обращения: 16.06.2025).
2. Внуков А.А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. М.: Издательство Юрайт, 2024. 161 с.
3. Зенков А.В. Информационная безопасность и защита информации: учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. М.: Издательство Юрайт, 2025. 107 с.

4. Комаров И.М. Криминалистические аспекты информационной безопасности досудебного производства // Научные ведомости. 2008. №8(48). С. 100.
5. Нестеров С.А. Информационная безопасность: учебник и практикум для академического бакалавриата / С. А. Нестеров. М.: Издательство Юрайт, 2019. 321 с.
6. Суворова Г.М. Информационная безопасность: учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. М.: Издательство Юрайт, 2025. 277 с.

Arakelyan. A.G.
Student
North-Caucation Federal University
(Stavropol, Russia)
Ovcharenko I.N.
Associate Professor of the Department of Criminal Law and Procedure
North-Caucation Federal University
(Stavropol, Russia)

FORENSIC ASPECTS OF ENSURING INFORMATION SECURITY AND PROTECTION OF INFORMATION

Abstract: *The work is devoted to the analysis of forensic aspects of ensuring information security and protection of information within the framework of pre-trial proceedings. The absence of a stable definition of the concept of information security in forensic science is noted, which complicates its normative and applied use in evidentiary activities. The theoretical and practical grounds for integrating the principles of information protection into the structure of criminal prosecution are revealed. The features of using forensic tools for the purpose of protecting evidentiary information from loss, distortion and unauthorized access are considered.*

The importance of an interdisciplinary approach in developing effective methods for recording and storing digital traces is emphasized. The need to systematize the conceptual apparatus and develop uniform standards that ensure the reliability and admissibility of information obtained during the investigation is substantiated.

Key words: *forensics, information security, information protection, evidence, forensic tools, data security.*