действия могут нанести ущерб национальной безопасности Республики Беларусь Наличие корыстного мотива, хотя и не является обязательным для квалификации преступления, может существенно повлиять на окончательное решение суда и определение меры наказания.

Таким образом, особенности расследования государственной измены в форме шпионажа заключаются в необходимости комплексного подхода, включающего как детальное изучение действий подозреваемого, так и взаимодействие с международными структурами. Успешное расследование зависит не только от сбора и анализа доказательств, но и от способности выявить и пресечь потенциальные угрозы для национальной безопасности, что является основополагающей задачей в условиях современных вызовов.

Понизович Д. А.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕХНИЧЕСКИЕ СРЕДСТВА В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ

Понизович Дмитрий Александрович, курсант 3 курса Академии Министерства внутренних дел Республики Беларусь, г. Минск, Беларусь, ponizovich1111@gmail.com

Научный руководитель: преподаватель Беломытцев Н. Н.

В условиях быстрого развития информационных технологий правоохранительные органы сталкиваются с новыми вызовами и возможностями. Разработка и внедрение новых технологий и технических средств в правоохранительной деятельности является ключевым фактором повышения эффективности и результативности борьбы с преступностью в современных условиях. Появление цифровых технологий связи, анализа данных и наблюдения изменило работу правоохранительных органов, включая расследование преступлений и взаимодействие с обществом.

Под современными информационными технологиями следует понимать систему операций, направленных на сбор, хранение, обработку и передачу информации по каналам связи посредством использования компьютерных технологий.

На текущий момент наблюдается активное внедрение технологий для автоматизации процессов, повышения прозрачности и улучшения взаимодействия с гражданами. Однако с ростом цифровизации возникают и новые угрозы, включая киберпреступность и утечку данных, что требует от правоохранительных органов адаптации и совершенствования существующих подходов. Эти угрозы и вызовы цифровой эпохи требуют не только совершенствования подходов к расследованию, но и внедрения новых инструментов, позволяющих более эффективно работать с большими объемами данных. Особое внимание уделяется созданию автоматизированных систем для хранения и обработки информации, специального хранилища (автоматизированной поисковой системы), которое помогло бы

систематизировать информацию, улучшить эффективность выполнения задач правоохранительных органов, а также предоставить доступ к данным сведениям всех уполномоченных на это и заинтересованных лиц.

Значительно повышает эффективность и качество выполнения возложенных на правоохранительные органы обязанности создание систем учетов, которые используются для регистрации информации о совершенном преступлении, о личности виновного лица, способе, месте, времени совершении преступления и т. п. Криминалистические учеты представляют собой результат деятельности уполномоченных лиц в рамках накопления, обработки и использования криминалистически значимой информации для расследования преступлений. Разработаны и внедрены в эксплуатацию информационные системы, охватывающие различные аспекты правоприменительной деятельности, включая хранение паспортных данных, учет нарушений правил дорожного движения, ведение банков данных о правонарушениях, а также регистрацию населения.

Процессы цифровизации оказывают значительное влияние на развитие экспертной деятельности, расширяя ее возможности и актуализируя новые направления. На практике активно развиваются различные виды судебных экспертиз, позволяющих должностным лицам получать специализированную информацию. Классические направления, такие как судебно-медицинская экспертиза, позволяют установить причину и время смерти, трасологическая экспертиза помогает определить механизм оставления следов, а дактилоскопическая экспертиза – идентифицировать личность по отпечаткам пальцев. Современные технологии, включая робототехнику и искусственный интеллект, усиливают точность и скорость этих процессов.

В то же время стремительная цифровизация и рост киберпреступлений формируют спрос на новые виды экспертиз (гендерная, религиоведческая, экологическая, этическая.), в том числе компьютерно-техническую экспертизу. Она позволяет анализировать цифровые следы, программное обеспечение, а также электронные устройства, что открывает новые горизонты в расследовании преступлений, связанных с компьютерно-информационной деятельностью и в сети Интернет.

Перспективы использования информационных технологий в правоохранительной деятельности включают развитие интегрированных систем мониторинга, применение алгоритмов машинного обучения для анализа криминогенной ситуации и расширение возможностей сотрудничества между различными государственными и частными структурами.

В заключение хотелось бы отметить, что информационные технологии и современные технические средства играют ключевую роль в повышении эффективности правоохранительной деятельности. Цифровизация изменяет методы сбора, анализа и обработки данных, открывая новые возможности для предотвращения преступлений и улучшения взаимодействия с гражданами. Активное использование интегрированных систем мониторинга и алгоритмов машинного обучения уже сегодня помогает эффективно бороться с киберугрозами и другими современными вызовами. Вместе с тем

внедрение этих технологий требует соблюдения правовых норм и защиты личных данных. В будущем ожидается дальнейшая интеграция IT-решений, что повысит возможности для раскрытия и предотвращения преступлений в условиях цифровой трансформации общества.

Секушенко С. И.

ВИКТИМОЛОГИЯ ЦИФРОВОЙ ПРЕСТУПНОСТИ

Секушенко Снежана Игоревна, студентка 3 курса Белорусского государственного университета, г. Минск, Беларусь, snezhana.sekushenko.2004@mail.ru

Научный руководитель: канд. юрид. наук, доцент Красиков В. С.

Инновационная политика государства, основанная на стратегиях развития высокотехнологичных секторов, поддерживает глобальные технологические тренды, а также приоритетные для страны отрасли развития. Все это приводит к появлению определенных изменений в обществе. Так, процесс информатизации общества вызван внедрением информационных технологий (IT) во все сферы деятельности человека. Вместе с тем криминальная статистика свидетельствует о том, что с внедрением новых технологий меняются и сферы преступной активности. Так, если 15-20 лет назад угрозу представляла уличная преступность, вызывал опасение уровень регистрируемых преступлений в общественных местах, то сегодня большая масса противоправных деяний совершается удаленным способом с использованием информационно-коммуникационных технологий, интернета и средств мобильной связи. Проводимые социолого-виктимологические опросы фиксируют рост виктимизации от преступлений, совершенных дистанционным способом. Такой вид дистанционной преступной деятельности, посягающей на приватность (конфиденциальность), единство (целостность) и открытость данных и информационных систем, получил название «киберпреступность». В научном сообществе к киберпреступлениям в широком смысле относят общественно опасные деяния, посягающие, помимо компьютерных систем, на иные охраняемые законом объекты, рассматриваются новые подвиды киберпреступности.

В соответствии с соглашением стран – участнц СНГ в борьбе с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 г.) не используется термин «киберпреступность», а дается определение преступления в сфере компьютерной информации как уголовно наказуемого деяния, предметом посягательства которого является компьютерная информация. На данный момент это определение присутствует только в доктрине.

Причиной большинства совершенных преступлений становилось халатное отношение пользователя к своим личным данным в сети. Таким образом, роль потерпевшего при совершении киберпреступлений трудно переоценить. Учение о жертве преступления исследует поведение разного рода лиц, пострадавших от преступлений. Интересным, на наш взгляд,