Т. 11. №6 2025
https://doi.org/10.33619/2414-2948/115

УДК 343.983 https://doi.org/10.33619/2414-2948/115/60

ХАРАКТЕРИСТИКИ И СВОЙСТВА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК СРЕДСТВА СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ

***©Голобородько И. Л.**, канд. юрид. наук, Кыргызско-Российский славянский университет, г. Бишкек, Кыргызстан*

CHARACTERISTICS AND PROPERTIES OF COMPUTER INFORMATION AS A MEANS OF COMMITTING A CRIME

***©Goloborodko I.**, Ph.D., Kyrgyz-Russian Slavic University, Bishkek, Kyrgyzstan*

Аннотация. Внедрение современных технологий, таких как искусственный интеллект и машинное обучение, открывает новые возможности для автоматизации процессов обнаружения и предотвращения киберугроз. Системы анализа поведения, основанные на этих технологиях, способны выявлять аномальную активность в сети и оперативно реагировать на потенциальные инциденты. Однако, применение данных технологий также требует особого внимания к вопросам конфиденциальности и защиты персональных данных. В условиях глобализации и увеличения числа трансграничных информационных потоков, важным становится международное сотрудничество в сфере информационной безопасности. Обмен опытом, разработка общих стандартов и протоколов, а также совместные усилия по борьбе с киберпреступностью позволяют эффективно противостоять угрозам, имеющим международный характер.

Abstract. The introduction of modern technologies such as artificial intelligence and machine learning opens up new opportunities for automating the processes of detecting and preventing cyber threats. Behavior analysis systems based on these technologies are capable of detecting abnormal online activity and responding promptly to potential incidents. However, the use of these technologies also requires special attention to privacy and personal data protection issues. In the context of globalization and the increasing number of cross-border information flows, international cooperation in the field of information security is becoming important. The exchange of experience, the development of common standards and protocols, as well as joint efforts to combat cybercrime make it possible to effectively counter threats of an international nature.

Ключевые слова: информационная безопасность, преступления, кибербезопасность, уголовный кодекс, защита, государство, общество.

Keywords: information security, crimes, cybersecurity, criminal code, protection, state, society.

В условиях цифровой трансформации общества, когда информационные технологии проникают во все сферы деятельности, обеспечение информационной безопасности становится критически важным элементом стабильного функционирования государства и экономики. Утечка конфиденциальных данных, кибератаки и другие виды информационных угроз могут привести к серьезным финансовым потерям, репутационному ущербу и даже дестабилизации политической обстановки. Анализ существующих подходов к информационной безопасности показывает, что универсального решения, пригодного для

Т. 11. №6 2025
https://doi.org/10.33619/2414-2948/115

всех организаций и систем, не существует. Каждая система имеет свои уникальные особенности и уязвимости, которые необходимо учитывать при разработке стратегии защиты. Поэтому требуется комплексный подход, включающий в себя как технические, так и организационные меры. Важным аспектом является постоянное совершенствование системы защиты, мониторинг новых угроз и уязвимостей, а также обучение персонала. Необходимо создавать культуру информационной безопасности, при которой каждый сотрудник осознает свою ответственность за защиту информации и соблюдает установленные правила и процедуры. Только в этом случае можно обеспечить эффективную защиту информационных систем от современных угроз. Необходимо отметить, что компьютерная информация, как предмет преступления, обладает рядом специфических характеристик. Во-первых, она существует в электронной форме, что делает ее уязвимой для несанкционированного доступа, копирования, изменения или уничтожения. Во-вторых, компьютерная информация часто хранится и передается через компьютерные сети, что расширяет географию совершения преступлений и затрудняет их расследование. В-третьих, преступления в сфере компьютерной информации могут быть совершены с использованием различных технических средств и методов, таких как вирусы, троянские программы, хакерские атаки и т. д. В качестве средства совершения преступлений компьютерная информация может использоваться для самых разных целей: от хищения денежных средств и интеллектуальной собственности до распространения вредоносного контента, и совершения террористических актов. Компьютеры и информационные технологии стали неотъемлемой частью многих преступных схем, позволяя злоумышленникам действовать более эффективно и оставаться анонимными.

Таким образом, компьютерная информация играет важную роль в современной преступности, как в качестве объекта посягательств, так и в качестве инструмента совершения преступлений. Борьба с преступлениями в сфере компьютерной информации требует комплексного подхода, включающего в себя разработку эффективного законодательства, применение современных технических средств и методов, а также повышение осведомленности граждан о рисках, связанных с использованием информационных технологий. Конфиденциальность самый проработанный аспект информационной безопасности. Конфеденциальность информации это свойство информации быть известной и доступной только правомочным субъектам системы [1].

Угроза конфиденциальности (угроза раскрытия) - это угроза, в результате реализации которой конфиденциальная или секретная информация становится доступной лицу, группе лиц или какой-либо организации, которой она не предназначалась. В литературе секретной обычно называют информацию, относящуюся к разряду государственной тайны, а конфиденциальной – персональные данные, коммерческую тайну [2].

Необходимо отметить, что преступления в сфере компьютерной информации обладают высокой степенью латентности. Зачастую, потерпевшие не осознают факта совершения в отношении них преступления, либо не желают предавать его огласке, опасаясь негативных последствий для своей репутации или коммерческой деятельности. При этом, важно учитывать, что развитие информационных технологий не стоит на месте, появляются новые виды компьютерных преступлений, требующие адекватного реагирования со стороны законодателя. В связи с этим, уголовное законодательство в сфере кибербезопасности должно постоянно совершенствоваться и адаптироваться к новым вызовам и угрозам.

Следует подчеркнуть, что борьба с преступлениями в сфере компьютерной информации требует комплексного подхода, включающего в себя совершенствование законодательства, развитие технических средств защиты информации, повышение уровня

осведомленности граждан о киберугрозах и активизацию международного сотрудничества в данной области. Только совместными усилиями можно обеспечить эффективную защиту компьютерной информации и минимизировать риски, связанные с ее неправомерным использованием.

При рассмотрении данного института необходимо уделить внимание преступлениям, содержащимся в главе 40 «Преступления против кибер-безопасности» (ст. 319-322 УК КР). Так, глава 40 Уголовного кодекса Кыргызской Республики посвящена охране исключительно информации, расположенной на особом носителе – электронном. Другими словами, информация, сосредоточенная на бумажном, например, носителе, становится предметом других преступлений. Действительно, отсутствует четкий критерий разграничения общественной опасности между преступлениями в сфере компьютерной информации и традиционными преступлениями, связанными с бумажными документами. Однако, на наш взгляд, помещение данных преступлений в раздел о общественной безопасности оправдано. Это обусловлено потенциально масштабными последствиями таких действий, затрагивающими не только отдельных лиц, но и функционирование критически важных систем общества. Особая значимость электронного документооборота и компьютерной информации в целом, делает их уязвимыми целями для злоумышленников. Нарушение целостности или доступности такой информации может привести к серьезным экономическим потерям, нарушению работы государственных органов, а также к угрозе национальной безопасности.

Таким образом, квалификация преступлений в сфере компьютерной информации как посягательств на общественную безопасность и общественный порядок представляется обоснованной, отражая повышенную степень общественной опасности, связанную с использованием современных информационных технологий в преступных целях. Необходима дальнейшая разработка критериев разграничения степени общественной опасности, с учетом специфики киберпреступлений. Поэтому охрана компьютерной информации в уголовном кодексе в рамках самостоятельного объекта уголовно-правовой охраны, признание компьютерной информации предметом компьютерных преступлений вполне оправдано.

Учитывая стремительный рост информационных технологий и их проникновение во все сферы общественной жизни, посягательства на компьютерную информацию приобретают все большую общественную опасность. Это обусловлено тем, что компьютерная информация является основой функционирования многих систем, включая финансовые, транспортные, энергетические и другие жизненно важные инфраструктуры.

Несанкционированный доступ, модификация, уничтожение или блокирование компьютерной информации может привести к серьезным последствиям, таким как финансовые потери, нарушение работы критически важных систем, утечка конфиденциальной информации, нарушение прав граждан и организаций.

В связи с этим, уголовно-правовая охрана компьютерной информации является необходимым условием обеспечения безопасности информационного общества и защиты прав и законных интересов граждан, организаций и государства. Совершенствование законодательства в этой сфере, а также эффективное правоприменение являются важными задачами государства в целях противодействия преступлениям в сфере компьютерной информации.

По мнению А. В. Наумова и других авторов, преступления в сфере компьютерной информации – это совершенные умышленно, общественно опасные деяния, направленные на установленный законом порядок обращения компьютерной информации или нормальное

функционирование (эксплуатацию) информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления и оконечного оборудования [3].

В соответствии с расположением данных преступлений в УК КР, их родовым объектом следует считать общественные отношения в сфере общественной безопасности и общественного порядка. Важность правильного определения предмета компьютерного преступления обусловлена тем, что от этого зависит квалификация деяния и, как следствие, справедливость наказания. Если компьютерная информация является лишь средством совершения преступления, то ответственность должна наступать за преступление, направленное на основной объект посягательства (например, хищение имущества с использованием компьютерных технологий). В тех же случаях, когда преступление непосредственно направлено на компьютерную информацию, ответственность должна наступать за компьютерное преступление. Сложность заключается в том, что грань между использованием компьютерной информации как средства и посягательством на нее как на самостоятельный объект часто бывает размытой. Например, несанкционированный доступ к компьютерной информации, содержащей коммерческую тайну, может быть квалифицирован как компьютерное преступление, если целью было получение доступа к информации, или как преступление против экономической деятельности, если целью было использование информации для получения конкурентного преимущества. Таким образом, при квалификации компьютерных преступлений необходимо тщательно анализировать все обстоятельства дела, чтобы установить, какой объект является основным, а какой – факультативным. Это позволит избежать ошибок в квалификации и обеспечить справедливое наказание за совершенное преступление.

Преступные посягательства все чаще направлены не только на саму компьютерную информацию, но и посредством воздействия на нее на иные блага: электронные средства платежа, иное имущество, государственную или банковскую тайну, объекты военного, жизнеобеспечивающего значения, а также на интересы отдельных личностей (жизнь и здоровье, личную неприкосновенность, собственность, интеллектуальную собственность и т.п.). Поэтому весьма актуальным является вопрос о том, является ли компьютерная информация предметом преступления или выступает в качестве орудия или средства совершения преступного посягательства.

В последнее время все более актуальным в уголовно-правовой науке является рассмотрение вопросов уголовной ответственности за преступления против компьютерной информации, а также за преступления, совершенные при помощи компьютерной информации. Тем не менее, теоретических и практических проблем в сфере квалификации компьютерных преступлений, в частности в сфере определения предмета данных посягательств, остается еще значительное количество. Поэтому, уголовное законодательство в данной части требует дальнейшего изучения и обновления. Это необходимо для совершенствования не только теории, но и правоприменительной практики. Исходя из названия гл. 40 УК КР, где сосредоточены так называемые «кибер-преступления», их предметом должна выступать компьютерная информация. Компьютерная информация — это сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Борьба с преступлениями в сфере компьютерной информации осуществляется в первую очередь ст. 319-322 УК КР в гл. 40 «Преступления против кибер-безопасности». Выделение самостоятельного объекта в рамках гл. 40 УК КР вполне оправдано современным развитием общества.

Т. 11. №6 2025
https://doi.org/10.33619/2414-2948/115

Вопрос о месте компьютерной информации в структуре преступления является дискуссионным в современной уголовно-правовой доктрине. Традиционно, предметом преступления признаются материальные объекты внешнего мира, на которые непосредственно направлено преступное деяние. В контексте компьютерных преступлений, компьютерная информация обладает специфической природой, являясь нематериальным активом, представленным в цифровой форме. С одной стороны, в случаях, когда целью преступления является непосредственное завладение, уничтожение, модификация или блокирование компьютерной информации, она, безусловно, выступает в качестве предмета преступления. С другой стороны, когда компьютерная информация используется лишь как инструмент для совершения иных преступлений, например, хищения денежных средств с банковского счета, она играет роль орудия или средства совершения преступления.

Разграничение компьютерной информации как предмета и как средства преступления имеет важное практическое значение для квалификации содеянного и назначения наказания. В первом случае, состав преступления может быть предусмотрен специальными статьями уголовного кодекса, посвященными компьютерным преступлениям. Во втором случае, квалификация осуществляется по статьям, предусматривающим ответственность за преступления против иных объектов, с учетом использования компьютерной информации в качестве средства совершения преступления. Таким образом, при квалификации деяний, связанных с компьютерной информацией, необходимо учитывать, что последняя может выступать не только как предмет, но и как средство совершения преступления. Это означает, что следует тщательно анализировать мотивы и цели злоумышленника, а также последствия его действий для различных сфер общественных отношений. Например, если целью злоумышленника является получение доступа к банковским счетам с целью хищения денежных средств, то компьютерная информация (логины, пароли, номера счетов) выступает средством совершения кражи или мошенничества. В этом случае квалификация должна производиться по соответствующим статьям уголовного закона, предусматривающим ответственность за эти преступления, а не только за неправомерный доступ к компьютерной информации. В тех случаях, когда умысел виновного направлен на нарушение государственной тайны, коммерческой тайны или иной охраняемой законом информации, квалификация должна учитывать специфику этих отношений и предусматривать ответственность за разглашение, утрату или использование таких сведений. При этом компьютерная информация выступает лишь инструментом для достижения преступной цели.

В частности, следует обратить внимание на случаи использования компьютерной информации для совершения мошенничества, вымогательства, клеветы, распространения наркотиков и других преступлений. Во всех этих ситуациях компьютерная информация выступает не как объект посягательства, а как средство совершения преступления против иных, традиционных объектов уголовно-правовой охраны. Усиление ответственности за преступления, совершенные с использованием компьютерной информации как орудия, должно сопровождаться разработкой четких критериев и методик определения размера ущерба, причиненного такими преступлениями. Это позволит судам более обоснованно назначать наказание и обеспечивать возмещение причиненного вреда.

Предлагаемые изменения в уголовном законодательстве потребуют от правоприменительных органов повышения квалификации в области информационных технологий и кибербезопасности. Необходимо обеспечить обучение следователей, прокуроров и судей современным методам расследования и рассмотрения дел, связанных с использованием компьютерной информации в преступных целях.

В заключение, обеспечение информационной и кибербезопасности в эпоху цифровой трансформации – это непрерывный процесс, требующий постоянного внимания, инвестиций и адаптации к меняющимся условиям. Только комплексный и многоуровневый подход, сочетающий в себе передовые технологии, организационные меры и международное сотрудничество, позволит эффективно защитить информационные ресурсы от современных угроз. В конечном итоге, совершенствование уголовного законодательства в данной сфере позволит создать более эффективную систему противодействия преступности в цифровой среде и обеспечить надежную защиту прав и законных интересов граждан, организаций и государства.

Список литературы:

1. Малюк А. А., Полянская О. Ю. Комментарии к доктрине информационной безопасности Российской Федерации. М.: Горячая линия–Телеком, 2018. С. 8.
2. Нестеров С. А. Основы информационной безопасности. СПб.: Лань, 2022.
3. Наумов А. В., Кибальник А. Г., Антонян Е. А. Уголовное право. Т 2. Особенная часть. М., 2018. С. 134.

References:

1. Malyuk, A. A., & Polyanskaya, O. Yu. (2018). Kommentarii k doktrine informatsionnoi bezopasnosti Rossiiskoi Federatsii. Moscow. (in Russian).
2. Nesterov, S. A. (2022). Osnovy informatsionnoi bezopasnosti. St. Petersburg. (in Russian).
3. Naumov, A. V., Kibal'nik, A. G., & Antonyan, E. A. (2018). Ugolovnoe pravo. 2. Osobennaya chast'. Moscow. (in Russian).

Работа поступила
в редакцию 09.04.2025 г.

Принята к публикации
17.04.2025 г.

Ссылка для цитирования:

Голобородько И. Л. Характеристика и свойства компьютерной информации как средства совершения преступления // Бюллетень науки и практики. 2025. Т. 11. №6. С. 490-495. https://doi.org/10.33619/2414-2948/115/60

Cite as (APA):

Goloborodko, I. (2025). Characteristics and Properties of Computer Information as a Means of Committing a Crime. *Bulletin of Science and Practice, 11*(6), 490-495. (in Russian). https://doi.org/10.33619/2414-2948/115/60