

ДАЛЕЛОВ Мухадин Леонович,
старший преподаватель (служащий) кафедры
информационных технологий и специальной техники ОВД,
e-mail: mail@law-books.ru

ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК ОСОБЫЙ ВИД ПРОТИВОПРАВНЫХ ДЕЯНИЙ

Аннотация. Современное развитие технологий ИИ открывает новые возможности для улучшения безопасности и правопорядка, одновременно возникают новые вызовы, связанные с возможностью его использования в противоправных целях во вред обществу и отдельным лицам.

Также немаловажную роль играет развитие направления кибербезопасности, поскольку рост числа кибератак требует усиленного внимания к вопросам информационной безопасности. Разработка национальных стандартов и законов направлена на защиту критической инфраструктуры и персональных данных граждан.

Ключевые слова: кибербезопасность, кибератака, информационная безопасность, защита инфраструктуры, персональные данные граждан.

DALELOV Mukhadin Leonovich,
Senior Lecturer (Employee) Department
of Information Technology and Specialized Equipment,
Department of Internal Affairs

CRIMES COMMITTED IN THE SPHERE OF COMPUTER INFORMATION AS A SPECIAL TYPE OF UNLAWFUL ACTS

Annotation. The modern development of AI technologies opens up new opportunities for improving security and law enforcement, while simultaneously raising new challenges related to the potential for its use for illegal purposes to the detriment of society and individuals.

The development of cybersecurity also plays a significant role, as the growing number of cyberattacks requires increased attention to information security issues. The development of national standards and laws is aimed at protecting critical infrastructure and citizens' personal data.

Key words: cybersecurity, cyberattack, information security, infrastructure protection, citizens' personal data.

Активное внедрение современных ИКТ способствует ускорению темпов экономического роста, повышению уровня благосостояния граждан и укреплению позиций России на международной арене.

Между тем, любые значительные преобразования в социальной, политической, экономической сферах общественной жизни неизбежно порождают противоправные явления, злоупотребления правом, и как закономерное следствие, изменение правового поля, усиление контроля со стороны государства, и разработки новых рычагов воздействия и механизмов для пресечения незаконной деятельности, минимизации ущерба,

привлечения к ответственности виновных лиц и недопущение совершения аналогичных деяний в дальнейшем.

При том, что значение информации, а соответственно и технологий её внедрения и распространения в обществе возрастает с каждым днём, тема правового регулирования данных отношений остается недостаточно изученной. Между тем, преступления в киберпространстве представляют собой качественно иной вид общественно опасных деяний, требующих специфических подходов как в области предупреждения, так и в сфере уголовно-правового воздействия [1, с.590].

Прежде всего, следует отметить специфику объекта посягательства, которым выступают информационные отношения, складывающиеся в процессе создания, обработки, накопления, хранения, поиска, распространения и использования информации. Непосредственным предметом преступного умысла в большинстве составов, по нашему мнению, будут являться оконечные устройства информатизации, компьютеры, смартфоны, сети, беспроводные соединения, серверы и прочие элементы информационной инфраструктуры [3].

Отметим, что преступления, совершаемые в сфере компьютерной информации, представляют собой особый вид противоправных деяний, направленных против информационной безопасности и конфиденциальности данных. Они получили широкое распространение благодаря развитию цифровых технологий и глобализации сети Интернет. Согласно российскому законодательству, подобные деяния регулируются главой 28 Уголовного кодекса Российской Федерации [2] (далее – УК РФ).

Субъектами преступлений в сфере компьютерной информации чаще всего выступают высококвалифицированные специалисты в области ИТ-технологий, хакеры, инсайдеры организаций, сотрудники компаний-конкурентов или злоумышленники, использующие анонимайзеры и ботнеты.

Кроме того, личность киберпреступника характеризуется сочетанием интеллектуальных качеств, как правило они обладают глубокими знаниями в области компьютерных технологий, импульсивностью, отстранённостью от жертв, а также для них зачастую характерен правовой нигилизм. Эти черты делают их крайне опасными для современного общества.

Также киберпреступники могут действовать в одиночку или в составе групп, где распределяются роли (например, «техподдержка», криптография, программирование). Важно отметить, что не существует единого, универсального портрета киберпреступника — характеристики могут существенно различаться в зависимости от конкретных обстоятельств и личности [4]. Но при этом преступной средой постоянно разрабатываются новые способы и средства противоправного воздействия, в том числе путем привлечения дополнительных лиц – посредников, таких как дропперы и скрипт-киддисы.

В качестве дропперов могут использоваться как вредоносные программы скрытого размещения другого программного обеспечения (обычно вирусов, троянов или шпионских программ) на устройстве жертвы, так и физическое лицо, которое помогает преступникам отмывать деньги или скрывать следы финансовых опера-

ций. Дроппер открывает банковские счета, регистрирует сим-карты, принимает переводы и выводит средства, действуя анонимно или подставляя чужое имя.

Несмотря на то, что скрипт-киддис вызывают интерес правоохранительных органов – сами по себе они в большинстве случаев не наносят широкого вредоносного воздействия, характеризующегося общественно опасным потенциалом, поскольку представляют собой молодых и неопытных пользователей цифровой среды, стремящихся продемонстрировать своё умение в области нарушений информационной безучастности и целостности объектов, используя готовые инструменты – эксплойты, вирусы, ботнеты и прочие автоматизированные решения [5].

Однако, они также могут быть вовлечены в широкую теневую сеть опытных хакеров, и выступать в качестве посредников.

Прежде всего, активное использование ИИ резко усиливает способности злоумышленников. Нейросети помогают создавать реалистичные фишинговые письма, вести глубокую социальную инженерию и даже осуществлять атаки через дипфейки.

Глобализация ИИ-технологий привела к снижению порога входа в киберпреступность, делая сложные атаки доступными широким слоям преступников. Складывающаяся тенденция предполагает дальнейшее углубление и модернизация атак с применением ИИ.

Преступники будут использовать ИИ для массовой генерации персонифицированных фишинговых писем, автоматического создания вредоносного ПО и ускорения атак через социальные сети и другие каналы коммуникации.

С другой стороны, субъекты совершения преступления используют всё более изощрённые техники, так, например, в последнее время хакеры участвовали в атаках через слабые звенья в цепочках поставок и партнерской экосфере.

Таким образом, маленькие компании, подрядчики и субподрядчики, имеющие низкую степень защиты, становятся идеальной точкой входа для атак на более крупные предприятия. Экспертами отмечается высокий риск, связанный с недостаточным вниманием к защите этих звеньев.

Список литературы:

[1] Рухлова М. А. Криминологические и уголовно-правовые меры борьбы с преступлениями в сфере компьютерной информации // Вестник науки. 2025. №6 (87).

[2] Белевитина Ю.В. О соотношении понятий «киберпреступность» и «преступления в сфере компьютерной информации». Инновационная наука. 2023. №1-2.

[3] Афанасьева О.Р. Гончарова Н.В. Шиян В.И. Криминология: учебник и практикум для академического бакалавриата. М.: Издательство Юрайт, 2017. 360с.

[4] Белоус А.И., Солодуха В.А. Основы кибербезопасности. Стандарты, концепции методы и средства обеспечения. Москва: Техносфера, 2021. 482 с.

[5] Геляхова Л.А., Машекуашева М.Х. Противодействие преступности в глобальном информационном пространстве: вопросы информационной безопасности. В сборнике: Экономическая безопасность личности, общества, государства: проблемы и пути обеспечения. Материалы всероссийской научно-практической конференции. Санкт-Петербург, 2025. С. 67-71.

References:

[1] Rukhlova M. A. Criminological and criminal legal measures to combat crimes in the field of computer information//Bulletin of Science. 2025. №6 (87).

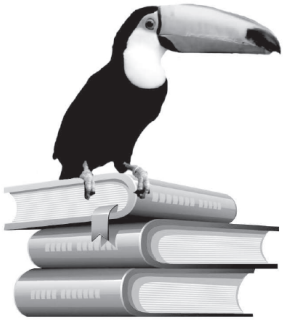
[2] Yu.V. Belevitina. On the relationship between the concepts of “cybercrime” and “crimes in the field of computer information. Innovative science. 2023. №1-2.

[3] Afanasyeva O.R. Goncharova N.V. Shiyan V.I. Criminology: textbook and workshop for academic undergraduate. M.: Yuright Publishing House, 2017. 360s.

[4] Belous A.I., Solodukha V.A. Cybersecurity fundamentals. Standards, concepts, methods and means of support. Moscow: Technosphere, 2021. 482 p.

[5] Gelyakhova L.A., Mashekuasheva M.Kh. Countering crime in the global information space: information security issues. In the collection: Economic security of the individual, society, state: problems and ways of provision. Materials of the All-Russian Scientific and Practical Conference. St. Petersburg, 2025. S. 67-71.





ЮРКОМПАНИ

www.law-books.ru

Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, E-Library.