чества оказывает влияние на состояние законности в целом в регионах и нельзя ли рассматривать преступления указанной категории в призме малозначительности.

Судебная практика о малозначительности взятки исходит из размера взятки (незначительности стоимости имущественной выгоды), отсутствия предварительной договоренности в ее получении, отсутствия нарушений служебных обязанностей должностного лица, отсутствия преступного результата.

Также необходимо отграничивать случаи правомерного вознаграждения служащего от взятки-подарка или взятки-благодарности.

Анализ Уголовного кодекса Российской Федерации позволяет сделать вывод о том, что минимальный размер взятки законодателем не установлен. В связи с изложенным считаем обоснованным включением мелкого взяточничества в статистические данные о совершении коррупционных преступлений.

Безусловно, изучение коррупционных преступлений является перспективной темой, нуждающейся в дальнейших научных исследованиях.

Молоков В.В.,

кандидат технических наук, доцент
Сибирский юридический институт МВД России (г. Красноярск)

Структура и динамика преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, в Сибирском федеральном округе

Согласно данным официальной статистики Министерства внутренних дел Российской Федерации, количество преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, демонстрирует тенденцию к росту[1]. Темпы прироста данных видов преступлений в России в период 2019-2021 гг. составили соответственно 54,8%, 73,4%, 1,4%. При этом можно констатировать, что данный тренд является ожидаемым, так как уровень развития цифровой экономики и вовлечения населения в сферу информационных коммуникаций в Российской Федерации на протяжении последних лет неуклонно повышается[2]. По своей сути цифровая экономика неизменно несет в себе потенциал криминологических рисков[3], связанных с угрозами комплексной безопасности личной, деловой, экономической, общественной и иной электронной информации, обрабатываемой с использованием компьютерных систем. По мере развития процессов цифровой трансформации общества и воздействия факторов внешних условий, каковым, например, является пандемия короновирусной инфекции, криминологические показатели отдельных видов и способов совершения преступлений варьируются. Присутствуют и региональные особенности, характерные для федеральных округов Российской Федерации[4]. Данный факт подтверждает системный характер наблюдаемых процессов современной индустриальной эпохи. Статистический и криминологический анализ состояния криминогенной обстановки в сфере обработки

[1] Статистика и аналитика // МВД России : официальный сайт. URL: https://мвд.рф/dejatelnost/statistics.

[2] Леднева О.В. Статистическое изучение уровня цифровизации экономики России: проблемы и перспективы // Вопросы инновационной экономики. 2021. Т. 11. № 2. С. 455-470.

[3] Ищук Я.Г., Пинкевич Т.В., Смольянинов Е.С. Цифровая криминология : учебное пособие. М.: Академия управления МВД России, 2021. С. 47-48.

[4] Невирко Д.Д., Рожков С.П., Мальков С.М. Преступность в Сибирском федеральном округе: общероссийские и региональные тенденции // Уголовное право. 2006. № 4. С. 118.

компьютерной информации и информационных технологий способствует глубокому пониманию происходящих процессов и развитию мер противодействия «технологичным» видам преступности.

По данным статистики зарегистрированных органами внутренних дел преступлений и отчетности Федеральной службы государственной статистики, на протяжении 2020-2021 гг. доля преступлений, совершаемых с использованием информационно-телекоммуникационных технологий (ИТТ), остается в среднем на уровне 25% в Российской Федерации и 23% в Сибирском федеральном округе (СФО). Таким образом, каждое четвертое преступление совершается с использованием ИТТ. Темп прироста таких преступлений в 2021 году в СФО демонстрирует небольшое снижение (-3,1%), тогда как в России он составляет (1,9%). Данный факт не является значимым, так как в массе всех разновидностей регистрируемых киберпреступлений присутствует волатильность и по отдельным показателям в СФО наблюдается их количественное превышение в разы. В частности, на территории СФО демонстрируют увеличение в три раза следующие виды преступлений: незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ), возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282 УК РФ). Регистрируются отсутствующие в 2020 г. преступления – склонение к совершению самоубийства или содействие совершению самоубийства (ст. 110.1 УК РФ), тогда как в Российской Федерации этот показатель остается неизменным на уровне 6 преступлений в год. Темпы прироста размера материального ущерба от рассматриваемых преступлений в 2021 г. составили в СФО 108,6%, в Российской Федерации – 73,6%.

Для сравнения ниже в таблице приведены данные о пяти наиболее растущих в 2021 г. видов преступлений, совершаемых с использованием ИТТ, на территории СФО и Российской Федерации.

Сибирский федеральный округ		Российская Федерация	
вид преступления	темп прироста, %	вид преступления	темп прироста, %
угроза убийством или причинение тяжкого вреда здоровью (ст. 119 УК РФ)	100	незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ)	156,6
мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ)	100	неправомерный оборот средств платежей ст. (187 УК РФ)	112,3
незаконный оборот сильнодействующих или ядовитых веществ в целях сбыта (ст. 234 УК РФ)	94,4	нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ)	63,6
неправомерный оборот средств платежей (ст. 187 УК РФ)	77,6	неправомерный доступ к компьютерной информации (ст. 272 УК РФ)	61,7
неправомерный доступ к компьютерной информации (ст. 272 УК РФ)	58,6	возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282 УК РФ)	59

Неизменными среди тенденций по использованию или применению средств совершения киберпреступлений являются: средства мгновенного обмена сообщениями (интернет-мессенджеры); социальные сети; электронные платежные системы; SIP-телефония; методы социальной инженерии. Как и в СФО, так и в Российской Федерации преобладает использование при совершении преступлений интернет-мессенджеров и SIP-телефонии (интернет-телефония).

Нельзя не затронуть преступления, связанные с мошенничеством, которые совершаются при использовании методов социальной инженерии. Темпы при-

роста мошенничеств (ст. 159 УК РФ), совершаемых с использованием ИТТ, в 2021 г. в СФО составили 9,7%, в Российской Федерации – 13,4%.

Факторами роста рассматриваемых преступлений кроме обозначенных ранее причин являются растущая популярность виртуализации личной жизни, доступность и простота использования информационно-телекоммуникационных технологий, вовлечение в сферу цифровых экономических отношений лиц, мало информированных и не подготовленных к возможным угрозам кибербезопасности, наличие средств анонимизации пользователей и массовое внедрение криптографических средств безопасности в сети Интернет.

Тем не менее динамика изучаемых видов преступности не дает оснований утверждать о преобладании в дальнейшем способов совершения, связанных исключительно с использованием ИТТ. Наблюдается некоторое плато, которое может дать как незначительный рост, так и стабилизацию. В этом заслуга органов внутренних дел, которые на текущий момент уделяют особое внимание противодействию подобным преступлениям, основываясь на концепции подготовки квалифицированных кадров в области информационно-телекоммуникационных технологий, и правильная государственная политика в сфере кибербезопасности. Не остаются в стороне и коммерческие компании, внедрение в деятельность современных систем обеспечения кибербезопасности способствует скорейшему расследованию киберинцидентов и противостоянию киберугрозам. Внедрение Роскомнадзором технических средств противодействия угрозам (ТСПУ) способствует ограничению к обороту противоправной информации и доступу к ресурсам, ранее использующимся для осуществления преступной деятельности, например сети Tor. Начало действия закона о «приземлении» иностранных ИТ-компаний[1] с целью соблюдения законодательства России обеспечит эффективный механизм для профилактики и раскрытия преступлений, совершаемых с использованием сети Интернет.

Резюмируя, можно утверждать, что преступления, совершаемые с использованием информационно-телекоммуникационных технологий, являются обратной стороной цифровой трансформации общества, но в системе преступность-население-государство приобретают регулируемые формы и не способны масштабно криминализировать складывающиеся электронные экономические, общественные и социальные коммуникации.

Щербич Л.А.,

кандидат юридических наук, доцент
Университет прокуратуры Российской Федерации (г. Москва)

Щербич А.Н.

Информационно-аналитическое управление ГУНК МВД России (г. Москва)

Цифровизация наркобизнеса

Наркоситуация в Российской Федерации остается достаточно сложной, о чем свидетельствует количество зарегистрированных преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ[2]. В 2021 г. их количество составило 179,7 тыс., в 2020 г. – 189,9 тыс.[3] На протя-

[1] О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации : Федеральный закон от 01.07.2021 № 236-ФЗ.

[2] По тексту приведены данные статистической отчетности, формируемой ФКУ «ГИАЦ МВД России».

[3] Раздел 1 формы № 1-МВ-НОН (код 171).