жизненный путь) / под ред. Б.Ф. Ломова, К.А. Абульхановой-Славской. – М. : Наука, 1980. – С. 7–17.

3. Анцыферова, Л.И. О динамическом подходе к психологическому изучению личности / Л.И. Анцыферова // Психол. журн. – 1981. – Т. 2, № 2. – С. 8–19.

4. Анцыферова, Л.И. Системный подход к изучению формирования и развития личности / Л.И. Анцыферова // Проблемы психологии личности / под ред. Е.В. Шороховой. – М. : Наука, 1982. – С. 140–148.

5. Анцыферова, Л.И. Личность в динамике: некоторые итоги исследований / Л.И. Анцыферова // Психол. журн. – 1992. – Т. 13, № 5. – С. 12–125.

6. Бодалев, А.А. Личность и общение / А.А. Бодалев. – М. : Междунар. пед. акад., 1995. – 328 с.

7. Завалова, Н.Д. Психические состояния человека в особых условиях деятельности / Н.Д. Завалова, В.А. Пономаренко // Психол. журн. – 1983. – Т. 4, № 6. – С. 92–105.

8. Иванова, Е.В. Некоторые аспекты изучения проблемы профессиональной деформации личности / Е.В. Иванова // Проблемы общей и прикладной психологии. – Ярославль, 2001. – С. 97–100.

9. Ковалев, В.П. Мотивационная сфера личности и ее динамика в процессе профессиональной подготовки / В.П. Ковалев, В.Н. Дружинин // Психол. журн. – 1982. – Т. 3, № 6. – С. 35–44.

10. Кон, И.С. Постоянство и изменчивость личности / И.В. Кон // Психол. журн. – 1987. – Т. 1, № 6. – С. 158–164.

11. Малыгина, О.В. Динамика личностного профиля женщин-сотрудниц уголовного розыска органов внутренних дел : дис. … канд. психол. наук : 19.00.03 / О.В. Малыгина. – Ярославль, 2008.

12. Малыгина, О.В. Специфика и динамика личностных особенностей сотрудников оперативных подразделений органов внутренних дел: гендерный аспект : монография / О.В. Малыгина. – Домодедово : ВИПК МВД России, 2001. – С. 4–83.

13. Социально-психологическая компетентность руководителя органов внутренних дел : учеб.-метод. пособие / М.Н. Марьин [и др.]. – М. : ЦОКР МВД России, 2005. – С. 3.

14. Поршуков, А.С. Личностные особенности сотрудников органов внутренних дел, назначаемых на должность руководителя / А.С. Поршуков // Нац. психол. журн. – 2020. – № 1 (37). – С.107–114.

15. Реан, А.А. Психология адаптации личности. Анализ. Теория. Практика / А.А. Реан, А.Р. Кудашев, А.А. Баранов. – СПб. : Прайм- ЕВРОЗНАК, 2006. – 479 с.

16. Родимушкина, О.В. Особенности прохождения женщинами службы в милиции : учеб. пособие / О.В. Родимушкина, М.В. Черетаева. – М. : ВНИИ МВД РФ, 1998.

17. Сысоева, Н.А. Особенности ценностных ориентаций женщин-сотрудников уголовного розыска / Н.А. Сысоева // Гендерные ценности и самоактуализация личности и малых групп XXI веке : материалы Междунар. симпозиума : Т. I. – М. ; К., 2004. – 255 с.

Дата поступления в редакцию: 21.03.2022

УДК 004:34

Е.Н. Мисун, А.А. Ластовский

ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ СОБЛЮДЕНИЯ ЦИФРОВОЙ ГИГИЕНЫ В ИНФОРМАЦИОННО-КОММУНИКАТИВНОМ ПРОСТРАНСТВЕ

Рассматриваются вопросы, связанные с организацией обучения цифровой гигиене граждан Республики Беларусь в связи с высоким темпом информатизации общества. Анализируются основные составляющие данного процесса и предлагается видение наиболее эффективной модели освоениями граждан основополагающих принципов «цифровой гигиены».

Ключевые слова: цифровая гигиена, цифровая безопасность, информационная безопасность, информационные технологии, информационно-коммуникативная деятельность, интернет.

E.N. Misun, A.A. Lastovsky

BASIC RULES FOR COMPLIANCE WITH DIGITAL HYGIENE IN THE INFORMATION AND COMMUNICATION SPACE

The issues related to the organization of digital hygiene training for citizens of the Republic of Belarus in connection with the high rate of informatization of society are considered. The main components of this process are analyzed and a vision of the most effective model for the development of citizens of the fundamental principles of 'digital hygiene' is proposed.

Keywords: digital hygiene, digital security, information security, information technology, information and communication activities, Internet, cybercrime, software, personal computer, gadget, digitalization (digitalization).

Стремительное развитие информационных технологий во всем мире и в Республике Беларусь в частности привело к существенному изменению реальности. Кардинальным образом изменились не только все сферы социально-бытовых отношений, но и окружающая действительность: мы не мыслим себя без мобильного телефона, не можем обойтись без персонального компьютера; окружили себя многочисленными техническими гаджетами и перепоручили им рутинную работу (роботы-пылесосы, голосовой сервис «Алиса», дистанционное управление бытовыми устройствами и т. д.).

Отдельно стоит отметить повсеместное и нарастающее использование различных форм дистанционного обслуживания. Республика Беларусь, как и все мировое сообщество, ориентирована на развитие и популяризацию безналичных расчетов, сопровождающихся увеличением количе-

ства устройств, осуществляющих финансовые транзакции, ростом числа пользователей всевозможных электронных платежных систем и сети Интернет (далее – интернет). Не последнюю роль сыграли последствия распространения коронавирусной инфекции COVID-19, в частности, переход в интернет-пространство многих сфер общественных отношений, включая удаленный режим работы, товарный и денежный обороты.

Сегодня в Беларуси почти все трудоспособное население страны так или иначе вовлечено в активности, связанные с вычислительными ресурсами, чаще всего осуществляемыми в интернете. Если в 2013 г. [1] удельный вес количества пользователей из числа граждан Республики Беларусь составлял 58,4 %, то в 2021 г. – уже 86,9 %. При этом заметное развитие интернет получил в сельской местности: удельный вес пользователей за указанный период вырос с 43,1 % до 76,9 %.

Значительно выросло и число организаций, использующих интернет. Если в 2011 г. лишь 9,2 % организаций сектора информационно-коммуникативных технологий имели доступ к интернету, то в 2018 г. этот показатель возрос до 30,1 %. Примерно такая же тенденция (с 9,6 % в 2011 г. до 38,4 % в 2020-м) наблюдается и относительно к организациям, не относящимся к сектору информационно-коммуникативных технологий [2].

Согласно данным аналитической платформы DataReportal, число интернет-пользователей в Беларуси по состоянию на январь 2022 г. составляло 8,03 млн человек (примерно 85 % от населения страны). Медианная скорость мобильного интернета равняется 10,33 Мбит/с (на 15,8 % выше, чем годом ранее), скорость фиксированного проводного подключения – 48,39 Мбит/с (на 24,8 % выше прошлогоднего показателя) [2].

В основном белорусы выходят в интернет с ноутбуков и компьютеров (57 %), однако доля этих устройств падает, в то время как смартфоны используются все чаще: их доля составляет 42 % (+13,2 % по сравнению с прошлым годом).

В список самых посещаемых белорусами сайтов вошли google.com, youtube.com и vk.com. Портал onliner.by идет на 6-м месте, торговая площадка kufar.by – на 9-м месте. Главный поисковик для белорусов – Google, он примерно в 3,5 раза популярнее своего ближайшего конкурента – «Яндекса». В Google белорусов больше всего интересуют погода и новости. Частыми были запросы в соцсети VK, «Одноклассники», связанные с решениями домашних заданий, картами, курсами валют и расписанием автобусов, а также фильмами и музыкой.

Количество мобильных подключений на начало 2022 г. в Беларуси составляло 11,64 млн, или 123,3 % от общего количества населения. За год

этот показатель вырос на 70 тыс. (+0,6 %). На широкополосные подключения (3G, 4G, 5G) приходится 76,4 %. В разрезе операционных систем больше всего трафика зафиксировано с Android (77,5 %), на 2-м месте – iOS (22,1 %), на 3-м – фирменная операционная система Samsung.

Количество белорусских пользователей соцсетей за год выросло на 450 тыс. и равняется 4,35 млн, или 46,1 % от общего количества населения. Примечательно, что 95,7 % выходят в соцсети с мобильных устройств.

Счет в банках и других финансовых организациях есть у 81,2 % населения, кредитными карточками владеют 18,7 % белорусов, дебетовыми – 70,6 %. Цифровые платежи за последний год совершали или получали 78,7 % населения, каждый третий сделал хотя бы одну покупку через интернет, 32 % пользовались интернет-банкингом, а 42 % оплачивали счета онлайн.

Как видим из приведенных статистических данных, в условиях столь стремительного развития цифровых технологий в Республике Беларусь и постоянно возрастающих объемов потоков цифрового контента все более актуальными становятся вопросы обеспечения безопасности.

Древнегреческий философ Гиппократ сказал: «Мы то – что мы едим!», подразумевая, что еда не только утоляет голод, но и влияет на здоровье и самочувствие. Сегодня это утверждение можно отнести не только к еде, но и к информации. Ведь потоки данных непосредственно влияют на наше ментальное здоровье.

Повышение общей информационной и компьютерной грамотности населения, включая обучение людей старшего и среднего возраста правилам защиты персональных данных, умению безопасной работы в интернете, наряду с подготовкой профессиональных кадров, определено в качестве одного из важнейших приоритетов по обеспечению информационной безопасности в Республике Беларусь. Наиболее предметно задачи повышения всеобщего уровня информационной безопасности населения раскрыты в принятой в 2019 г. Концепции информационной безопасности Республики Беларусь [3] (далее – Концепция) и направлены на обеспечение ее двух составляющих – информационно-психологической и информационно-технической.

Так, согласно п. 41 Концепции противодействие деструктивным информационно-психологическим воздействиям (распространению фальсифицированной, недостоверной и запрещенной информации) в первую очередь основывается на формировании у населения ответственного поведения в информационном пространстве, а также на продвижении общих правил коммуникации с едиными для физического мира и вир-

туального пространства правами и обязанностями участников информационных процессов.

В рамках борьбы с несанкционированными информационно-техническими воздействиями согласно п. 76 Концепции одним из приоритетных направлений деятельности уполномоченных государственных органов определена профилактика киберпреступности, основанная на популяризации среди населения, прежде всего молодежи, нетерпимости к асоциальному поведению в информационном пространстве, проведении разъяснительной работы в средствах массовой информации (СМИ) и интернета в целях формирования безопасной национальной информационной экосистемы.

Развитие информационных систем, а вслед за ними систем обеспечения защиты информации определило высокую частоту использования устойчивого словосочетания *«цифровая безопасность»*, или его синонимического родственника – *«цифровая гигиена»*.

К сожалению, большинство пользователей, вовлеченных в сферу информационно-коммуникативных отношений, имеют недостаточный уровень владения соответствующими компетенциями по обеспечению своей безопасности.

Многие считают, что технологии нейтральны, и пользуются ими, даже не задумываясь о том, как они устроены и на что влияют. Поэтому огромное количество пользователей интернета, слабо осведомленных об угрозах цифровой безопасности, представляют собой обширную, привлекательную и уязвимую целевую группу для злоумышленников. В интернете мы без тени сомнения сообщаем неизвестным лицам реквизиты банковских платежных карточек. А в реальном мире мы разве отдадим кошелек со всем содержимым первому проходимцу, который нас попросит об этом? Вопрос риторический…

Нас с детства учат различать добро и зло, обучают правилам поведения индивида в обществе, прививают навыки правильного поведения на дороге. А вот правилам поведения в цифровой среде не уделяется должное внимание. Основная проблема здесь заключается в том, что цифровая среда широкими массами серьезно не осознается и не формулируется в четко выстроенный поведенческий алгоритм.

Таким образом, в условиях цифрового мира понятие *«цифровая гигиена»* можно трактовать как *«обязательное следование ритуалам и правилам, направленным на обеспечение безопасности граждан при нахождении в цифровом пространстве»*. Если нарушить основополагающие правила «цифровой гигиены», можно столкнуться с крайне негативными последствиями: потерять доступ к важным аккаунтам, расстаться с деньгами, подхватить «вирус» и т. д.

Многие до сих пор не могут осознать, что, наряду с нашей личностью в реальном мире, в цифровом пространстве свою жизнь «отзеркаленно» проживает их цифровой клон. Он представляет собой совокупность цифровой информации о реальной личности, которая в той или иной степени оказалась общедоступной и была размещена в цифровой среде. Этот массив составляют:

информация о персоне, ставшая общедоступной и размещенная в цифровом пространстве: биографические данные (Ф.И.О., место проживания, полные сведения о семье, ближнем и дальнем круге общения, традиции и привычки членов семьи); социальный статус (место работы или учебы всех членов семьи, сведения об имеющемся в наличии имуществе);

мультимедийная информация: фото, видео- и аудиоматериалы; скриншоты личных переписок; передаваемые дистанционно текстовые документы, сохраненные/отмеченные в закладках публикации других интернет-пользователей и т. д.

программно-технический блок: электронные почтовые ящики, аккаунты в социальных сетях, личные кабинеты интернет-сайтов, авторизированное пользование онлайн-ресурсами (видеохостинги, форумы, базы данных, web-версии мессенджеров), онлайн-игры и т. д.

финансовая информация: использование интернет-банкинга, расчет на торговых площадках, оплата услуг посредством онлайн-сервисов, оформление карт лояльности, трансфер платежной информации третьим лицам.

Соединив вышеуказанные элементы воедино, можно получить вполне самодостаточный и узнаваемый облик, цифровой клон человека. Проанализировав информацию по этому «цифровому слепку», можно получить полное представление не только о личности человека, его привычках, интересах, предпочитаемом времяпровождении, но и узнать его место жительства, социальный статус, уровень жизни. Или получить доступ к его финансовой информации – вероятность успеха зависит от того, насколько щепетильно пользователь соблюдает правила «цифровой гигиены».

Если правила личной гигиены необходимы для приведения организма к социально-биологическому благополучию, то правила «цифровой гигиены» направлены на защиту нашего цифрового клона. Для приобретения необходимых базовых компетенций любой пользователь должен владеть определенным комплексом знаний и умений. Условно разделим их на несколько категорий: *аппаратно-техническая, программная, информационная грамотность*.

Остановимся на информационной грамотности. Информационная грамотность предполагает наличие навыков, необходимых для безопас-

ного использования информационно-коммуникативных технологий. В наиболее общем смысле информационная грамотность представляет собой набор компетенций, необходимых для получения, понимания, оценки, адаптации, генерирования, хранения и представления информации, используемой для повседневной жизни. Информационно грамотные люди обладают: критическим мышлением, умением анализировать информацию и использовать ее для самовыражения, способностью к созданию информации, готовностью быть информированным гражданином и профессионалом.

Автор термина «критическое мышление» – американский философ Джон Дьюи, который впервые использовал его в 1910 г. в книге под названием «Как мы мыслим» (впервые издана на русском языке уже в 1919 г. под названием «Психология и педагогика мышления») [4]. В данной работе, а затем и в последующих научных трудах, Дж. Дьюи именовал «критическое мышление» в различных вариантах: то как «рефлексивное мышление», то как «рефлексивную мысль» или даже просто как «мысль», «мышление» и даже «рефлексию». Это мышление он трактовал как активное, настойчивое, тщательное, применяемое в отношении всех форм информации. На сегодня равнозначность, а по сути дела, синонимичность этих терминов официально признана многими современными западными философами, педагогами и психологами.

Умение анализировать информацию и использовать ее для самовыражения является необходимым навыком работы в информационном пространстве. Анализ информации тесно связан с процессами ее восприятия и интерпретации.

Процесс восприятия неразрывно связан с каждым из важных психологических процессов: мышлением, речью, чувствами, волей. Образы восприятия как факты психической деятельности легко поддаются словесному описанию. Восприятие представляет целостное отражение предметов, ситуаций, явлений, возникающих при непосредственном воздействии физических раздражителей на рецепторные поверхности органов чувств [5, с. 200]. Интерпретация – объяснение какого-либо факта, явления посредством других известных фактов и явлений. Интерпретация – это также объяснение, суть которого заключается в том, что нечто, требующее объяснения, получает такое объяснение путем сведения неизвестного или непонятного (объясняемого) к известному и понятному (объясняющему) [6, с. 158]. Осуществляя процесс восприятия, мы формируем образы, которые интерпретируются и оказывают на человека позитивное либо негативное воздействие.

Зададимся вопросами, с какими основными рисками может столкнуться человек в информационной сфере, для чего необходимо постоянно совершенствовать навык работы и «жизни» в информационном пространстве?

Во-первых, это безопасность личных аккаунтов. Помним ли мы, сколько электронных ящиков создали за свою жизнь и реквизиты доступа к ним? Сколько аккаунтов и в каких соцсетях создали, какую информацию о себе размещали? В каких сервисах создавали личные кабинеты, вводили платежную информацию? А ведь все эти аккаунты и электронные ящики, доступ к которым уже может быть окончательно утрачен, являются мишенью непрекращающихся хакерских атак, осуществляемых в автоматическом режиме в формате времени 24/7 специальными программами. Подобрав пароль к аккаунту и получив доступ к нему, злоумышленники получат полный контроль над вашей страницей. От вашего имени они могут рассылать мошеннические просьбы перечислить деньги на телефон вашему списку друзей; изучать личные переписки и шантажировать подробностями о личной жизни или пикантными фотографиями; использовать персональные данные для совершения противоправных операций в интернете.

Пароль – своего рода замок, охраняющий ваше интеллектуальное имущество от преступных посягательств. Чем сложнее пароль – тем надежнее защита. Рекомендуется менять пароли не реже чем раз в полгода. При составлении нового пароля необходимо ориентироваться на количество 8–12 символов; в пароле должны присутствовать и буквы, и цифры; символы должны быть разного регистра; следует избегать повторения символов; пароль не должен содержать фрагментов вашей персональной информации (дата рождения, ваши Ф.И.О., кличка домашнего животного).

Но при этом нужно помнить, что степень безопасности любой системы определяется самым слабым звеном. Если мы используем 20-символьный пароль, представляющий собой сочетание случайных символов, а листок, на котором он записан, хранится в ящике стола, то сложность доступа определяется не возможностями по перебору всех вариантов, а лишь доступом к ящику.

Во-вторых, вызывает опасение увеличивающееся количество мошенничеств, совершаемых в интернете. В первую очередь, речь идет об использовании мошенниками метода социальной инженерии, получившего массовое распространение в последние годы в Республике Беларусь. Социальная инженерия – метод получения необходимого доступа к информации, основанный на особенностях психологии людей. Злоумышленники пытаются применить социальную инженерию, используя телефон, электронную почту и интернет. В основном мошенники

апеллируют к базовым эмоциям человека – страху, вине, обиде и т. д. Умело используя технологии социальной инженерии, мошенникам удается получить доступ к реквизитам банковских платежных карточек, денежным средствам. В условиях ограниченного времени потенциальной жертве предлагается быстро принять решение, ведь угрозе подвергаются их финансовые средства, близкие родственники. На сегодня известны такие формы «обмана», как вишинг, фишинг, смишинг, фарминг.

Так, например, вишинг реализуется по следующей схеме. Позвонив потенциальной жертве под видом работника банка или сотрудника правоохранительных структур, злоумышленники создают стрессовую ситуацию и под различными предлогами выведывают реквизиты доступа к банковскому расчетному счету жертвы для кражи денег, либо получают денежные средства непосредственно от самих жертв.

Существуют и иные мошеннические способы для получения доступа к платежным системам. Злоумышленники весьма изобретательны и регулярно совершенствуют свои преступные схемы, снижая уровень бдительности потенциальных жертв. Одной из последних преступных успешных схем является просьба одолжить на время телефон случайного прохожего с целью позвонить. Однако вместо звонка злоумышленник получает доступ к платежным инструментам и дистанционно открывает микрокредит на пользователя, а полученные средства выводят на свой счет.

В-третьих, негативное информационное воздействие. Интернет предоставил возможность в режиме реального времени следить за событием. Кроме того, он дал возможность каждому желающему стать медиапроектом, освещающим события под любым желаемым углом. Сегодня каждый блогер может позиционировать себя журналистом. Это, в свою очередь, существенно обесценило качество и достоверность информации, фактически превратив информацию в орудие пропаганды. Увеличилось количество фейковой информации, размещенной в интернете. Фейк может быть намеренным и ненамеренным, полным или частичным. Фейковым может быть контент практически любого вида: новость, изображение, видеоролик и даже аккаунт в социальных сетях. По сравнению с обычными новостями фейк распространяется гораздо быстрее благодаря вбросам. При этом среднее время жизни фейка значительно меньше – в среднем фейк живет 3–4 дня. Площадками для распространения фейков выступают:

квази-СМИ. Сайты, «изображающие» интернет-СМИ. Они распознаются по минимальному присутствию авторских материалов, а чаще всего состоят из новостей, автоматически собранных из других источников;

разовые страницы. Одноразовые сайты, состоящие из нескольких страниц, но имеющие вид СМИ, аналитического издания. Ссылки на

такую публикацию обычно приходят из соцсетей, со страниц, специально созданных для имитации «канала» несуществующего СМИ;

имитация известных СМИ. Одноразовые страницы, созданные для вброса, которые имитируют известные читателю СМИ, оформляются в дизайне и содержат логотипы известных новостных и аналитических сервисов.

Здесь стоит упомянуть и негативное взаимодействие с виртуальным собеседником. Анонимность в общении позволяет собеседнику по ту сторону экрана не только оставаться инкогнито, но и перевоплотиться полностью. Чувство анонимности и безнаказанности проявляет в людях порой самые низменные инстинкты, открывая им возможность вести себя по отношению к другим неподобающим образом. В этом и заключаются предпосылки удовлетворения своих низменных потребностей при общении между собеседниками («троллинг»), травли несовершеннолетних («кибербуллинг») и т. д.

В целом политика Республики Беларусь в области информатизации и развития цифровой грамотности населения соответствует мировой практике. Вместе с тем, очевидно, что с учетом активного использования населением цифровых технологий обучающие процессы, формирующие компетенции «цифровой гигиены», необходимо начинать уже в начальной школе. Отдельные вопросы информационной грамотности и «цифровой гигиены» могут прививаться уже в учреждениях дошкольного образования по аналогии с позитивно зарекомендовавшими себя программами МЧС и ГАИ по обучению детей стандартам безопасности, прежде всего в игровой форме. Кроме того, необходимо формировать соответствующие обучающие программы и для старшего поколения, используя для процесса обучения основам «цифровой гигиены» все доступные для этого возможности: информационные часы, факультативные занятия, единые дни информирования и т. д. Безусловно, следует и самостоятельно заботиться о своей безопасности. Как гласит народная мудрость, «спасение утопающего – дело рук самого утопающего». Поэтому каждому необходимо самостоятельно повышать свой уровень, ознакамливаясь с актуальной информацией в сфере противодействия киберпреступности. В частности, помогут в этом соответствующие разделы на официальном интернет-сайте МВД Республики Беларусь, а также официальные сообщества министерства в социальных сетях.

Список использованных источников

1. Удельный вес количества пользователей сети Интернет из числа граждан Республики Беларусь [Электронный ресурс] // Официальный интернет-сайт Национального статистического комитета Республики Беларусь. – Режим доступа:

http://dataportal.belstat.gov.by/Indicators/Preview?key=226247. – Дата доступа: 26.02.2022.

2. Распределение организаций по виду подключения к сети Интернет [Электронный ресурс] // Официальный интернет-сайт Национального статистического комитета Республики Беларусь. – Режим доступа: https://www.belstat.gov.by/ofitsialnaya-statistika/makroekonomika-i okruzhayushchaya-sreda/informatsionno-telekommunikatsionnye-tekhnologii/godovye-dannye/. – Дата доступа: 26.02.2022.

3. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета Безопасности Респ. Беларусь, 18 марта 2019 г., № 1 // Национальный правовой Интернет-портал Республики Беларусь, 20.03.2019, 7/4227. – Режим доступа: http://www.pravo.by. – Дата доступа: 26.02.2022.

4. Дьюи, Дж. Психология и педагогика мышления : пер. с англ. Н.М. Никольской / под ред. Н.Д. Виноградова. – М. : Изд. Товарищества «Мир», 1919. – 202 с.

5. Маклаков, А.Г. Общая психология : учеб. для вузов / А.Г. Маклаков. – СПб. : Питер, 2016. – 583 с.

6. Немов, Р.С. Психологический словарь / Р.С. Немов. – М. : Гуманитар. изд. центр «ВЛАДОС», 2007. – 560 с.

Дата поступления в редакцию: 18.03.2022

УДК 159.9:34

А.Н. Пастушеня

ПСИХОЛОГИЧЕСКИЙ АНАЛИЗ ПРЕСТУПЛЕНИЯ В КОНТЕКСТЕ ЕГО КРИМИНАЛИСТИЧЕСКОЙ И УГОЛОВНО-ПРАВОВОЙ ОЦЕНКИ

Представлен комплексный подход к психологическому анализу преступления, который имеет значение как для его раскрытия и расследования, так и для уголовно-правовой оценки его субъективной стороны. Изложены два возможных аспекта психологического анализа преступления: структурно-функциональный, представляющий раскрытие психологического механизма преступления, и процессный, выражающий описание развертывающегося во времени его генезиса. Психологический анализ охватывает такие элементы психологического механизма преступления, как восприятие субъектом обстоятельств ситуации, мотивообразование, целеполагание, исполнительную регуляцию, фоновое психическое состояние, внешние условия, личностную предрасположенность к совершению деяния.

Ключевые слова: психологический анализ преступления, психологический механизм преступления, психологический генезис преступления, личность преступника, готовность к совершению преступного деяния.

A.N. Pastushenya

PSYCHOLOGICAL ANALYSIS OF A CRIME IN THE CONTEXT OF ITS CRIMINALISTIC AND CRIMINAL-LEGAL ASSESSMENT

A comprehensive approach to the psychological analysis of a crime is presented, which is important both for its disclosure and investigation, and for the criminal legal assessment of its subjective side. Two possible aspects of the psychological analysis of the crime are described: structural and functional, representing the disclosure of the psychological mechanism of the crime, and process, expressing the description of its genesis unfolding in time. Psychological analysis covers such elements of the psychological mechanism of the crime as the subject's perception of the circumstances of the situation, motivation, goal setting, executive regulation, background mental state, external conditions, personal predisposition to commit an act.

Keywords: psychological analysis of the crime, psychological mechanism of the crime, psychological genesis of the crime, personality of the criminal, readiness to commit a criminal act.

В 70-х гг. прошлого столетия белорусский ученый А.В. Дулов в своем учебном пособии «Судебная психология» обосновал необходимость «психологического анализа преступной деятельности» при расследовании преступлений. Им обращено внимание на необходимость анализа «психологической структуры преступления», которая, как отмечал ученый, включает прогнозирование, планирование и совершение преступных действий, сокрытие следов преступления, охватывая при этом цель, способ, потребность, мыслительную деятельность [1, с. 202–203]. Безусловно, познание этих составляющих психической деятельности субъекта преступления, детерминирующей его преступное поведение, необходимо для реконструкции противоправного деяния с необходимой полной и достаточной точностью как для безошибочности установления субъекта преступления, точности воспроизведения объективной стороны, неотделимой от порождающей ее психической деятельности, так и для правильной оценки всех составляющих субъективной стороны преступления, включая оценку умысла либо неосторожности, мотивов, цели, психического состояния преступника, восприятия им обстоятельств ситуации, включая поведение потерпевшего. Все это имеет значение как в криминалистическом аспекте для раскрытия и расследования преступления, так и в уголовно-правовом, включая не только оценку субъективной стороны, но и обстоятельств, смягчающих и отягчающих ответственность, отдельные из которых имеют психологическую сущность.

Раскрытие особенностей психической деятельности субъекта, детерминирующей его преступное поведение (деяние) является важной науч-