наркотических средств, в том числе опиоидов, в округе на протяжении шести лет (2014-2019 гг.), при незначительном уменьшении количества пациентов, зарегистрированных с диагнозом «наркомания вследствие потребления опиоидов».

Дмитриева Т.В.
DOI 10.51980/2021_3_78

Московский государственный областной университет (г. Мытищи)

Цифровые технологии как инструмент современной преступности

Современный мир – это мир, в котором главенствуют информация и цифровые технологии. Человек XXI века не представляет свою жизнь без смартфонов, компьютеров и, главное, интернета. Мы находимся в активной стадии информационной революции[1] – ее цифровом этапе[2].

Основой этого этапа выступают «цифровые технологии». Термин «цифровые технологии» может использоваться в узком и широком смысле. В узком смысле – как основанная на методах кодировки и передачи информации дискретная система, позволяющая совершать множество разноплановых задач за кратчайшие промежутки времени[3]. В широком смысле это не отдельная сфера деятельности, но уклад жизни, новая основа для развития системы государственного управления, экономики, бизнеса, социальной сферы[4]. Цифровые технологии все больше внедряются и кардинально меняют все сферы нашей жизнедеятельности. Преступная деятельность также перемещается в интернет-пространство. Естественно, что увеличиваются и цифровые риски. Это касается как безопасности персональных и коммерческих данных, так и безопасности жизни человека.

Во Франции начала XIX века, наряду с увеличением роста городов и промышленных производств, произошел небывалый рост преступности. Одной из причин такого положения стало отсутствие в стране элементарной паспортизации граждан. Каждый человек был вправе представиться любым именем.

---

[1] От лат. revolution – поворот, переворот.

[2] Дмитриева Т.В. Цифровой этап информационной революции: сущность, предпосылки, тенденции // Вестник Тверского государственного университета. Серия «Философия». 2020. № 4.

[3] Романова Т. Цифровые технологии человечества. URL: turbo/fb.ru/s/article/335698/tsifrovyie-tehnologii---eto-buduschee-chelovechestva (дата обращения: 29.01.2021).

[4] Цифровые технологии. URL: https://mentalar.ru/cifrovye-texnologii/ (дата обращения: 29.01.2021).

Аналогичные процессы характерны и для информационной революции. В интернете также сложно выявить личность человека, совершившего преступное деяние, и, следовательно, найти такого правонарушителя.

По данным МВД России, число противоправных деяний, совершенных «с применением информационных технологий», увеличилось почти на 70%[1].

К сожалению, интернет-пространство слабо поддается законодательному регулированию, несмотря на существование целого Министерства цифрового развития, связи и массовых коммуникаций. Скорее всего, это вызвано тем, что написание и внедрение новых законодательных актов требует политической воли, времени и значительного финансирования. В то же время преступные группировки оперативно и творчески используют достижения научно-технического прогресса.

Сегодня мы часто встречаемся с понятием «киберпреступление», под которым понимается преступление, причиняющее вред разнородным общественным отношениям, совершаемое дистанционно, путем использования средств компьютерной техники, информационно-телекоммуникационных сетей и образованного ими киберпространства[2].

Какие угрозы несут в себе цифровые технологии?

Во-первых, это безопасность персональных данных человека. В настоящий момент сохранить информацию конфиденциальной[3], то есть «доверительной, не подлежащей огласке, секретной», практически невозможно, поскольку вся информация о нас есть в сети: начиная от паспортных данных, которые мы вводим, регистрируясь на портале государственных услуг, и заканчивая предпочтениями человека при покупке продуктов. Это не говоря о том, что наши банковские реквизиты существуют в компьютерных базах данных, которые официально закрыты, а неофициально могут быть приобретены на сайтах человеком, не имеющим на это никаких прав, но имеющим желание и средства. При столь простом доступе к информации сложно сохранить данные конфиденциальными. Поэтому мошенники с

---

[1] Сидоренко Е. По цифровым следам: в РФ раскрывается лишь четверть киберпреступлений. URL: https://iz.ru/962966/elena-sidorenko/po-tcifrovym-sledam-v-rf-raskryvaetsia-lish-chetvert-kiberprestuplenii (дата обращения: 27.01.2021).

[2] Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им. URL: https://rgup.ru/rimg/files/001Диссертация_ Простосердов_М.А. pdf (дата обращения: 26.01.2021).

[3] От лат. confidentia – доверие.

легкостью используют личные данные человека для заключения фиктивных сделок и проведения незаконных коммерческих операций.

По материалам регулярного исследования инсайдерских утечек информации из российских компаний, проведенного системой DeviceLock, обеспечивающей защиту корпоративной информации, в 2019 г. менее 2% персональных сведений россиян утекали через IT-специалистов. Пока число инцидентов невелико, но по объему похищенной информации на этот канал приходится до 30%. Остальные 98% утечек происходят из-за сотрудников других подразделений банков и компаний[1], но они не столь масштабны.

Во-вторых, во время пандемии многократно возросло количество мошеннических операций, связанных с куплей-продажей товаров в интернет-приложениях. Такие большие коммерческие площадки, как «Авито» или «Юла», вынуждены запрашивать большое количество подтверждений для регистрации товаров на сайтах и постоянно предупреждают потребителей о возможных мошенниках.

Еще сложнее сохранить коммерческую тайну крупным компаниям. Для обеспечения безопасности собственной деятельности они вынуждены тратить баснословные деньги. Из-за пандемии и перевода сотрудников на удаленную работу большое количество корпоративных данных попало под угрозу несанкционированного доступа вследствие неготовности компаний к столь глобальному процессу реорганизации работы.

По прогнозам экспертов международной компании ESET, в 2021 г. многие столкнутся с набирающей распространение преступной схемой безфайлового проникновения (так называемые программы-вымогатели)[2]. В 2021 г. подобные методы могут использоваться во все более сложных и крупномасштабных атаках, повышенному риску подвергнутся госучреждения, как обладающие наибольшим количеством персональных данных. Постепенно компании приобретают опыт и внедряют цифровые технологии, которые предотвращают атаки и создают устойчивые процессы резервного копирования быстрее, чем преступники создают новые программы.

В-третьих, невозможно обойти вниманием такое следствие цифровых технологий, как социальные сети, особенно их влияние на молодежь. Каждая социальная сеть выступает источником информации для потенциальных преступников, собирающих персональные

---

[1] От IT в сторонку: в 2019-м появился новый канал утечек личных данных. URL: https://news.mail.ru/society/39872927/?frommail=1 (дата обращения: 26.01.21).

[2] Тренды кибербезопасности-2021 по версии ESET: рост активности программ-вымогателей и атак с помощью безфайлового ПО. URL: http://www.itsec.ru/news/trendi-kiberbezopasnosti-2021-po-versii-eset (дата обращения: 29.01.21).

данные для использования в дальнейшем с целью обмана и мошенничества. Поэтому важно правильно выбрать сеть и настроить конфиденциальность собственного профиля, чтобы ограничить доступ других пользователей к публикуемой вами (и о вас) информации.

В этом отношении кое-что делается и на законодательном уровне. Так, 25 декабря 2020 г. Совет Федерации одобрил законопроекты, направленные на снижение иностранного влияния на россиян и отечественные компании[1]. Там вводится понятие «статус владельца информационного ресурса, причастного к нарушениям основополагающих прав и свобод человека и граждан Российской Федерации».

При определенных условиях могут быть заблокированы даже глобальные сети Facebook, YouTube, Twitter, Google. Соцсети обязали скрывать контент с оскорблениями власти и призывами к массовым протестам. А за клевету в Интернете теперь могут даже сажать в тюрьму.

Все чаще в нашем общении встречается понятие «кибербуллинг» – вид насилия в цифровой среде, реализуемый с помощью электронного текста (сообщений и комментариев). Наиболее страшным и нашумевшим примером кибербуллинга является жестокая игра «Синий кит», в которой детей склоняют к самоубийству. За последнее время правоохранители арестовали несколько десятков кураторов таких игр. При этом многие задержанные преступники отделались условными сроками заключения, так как доказать прямую связь между самоубийствами детей и деятельностью куратора сложно.

В-четвертых, Интернет активно используется наркопреступностью как средство предложения и распространения наркотиков. Интернет-пространство нуждается в правовом регулировании. Но не стоит забывать, что мы можем защитить себя и своих близких самостоятельно. Чтобы защитить ребенка от кибербуллинга, зачастую достаточно просто уделять ему больше внимания. Психологи утверждают, что ежедневное личностное общение с ребенком, хотя бы по 15 минут (без отвлечений на телефон и телевизор), позволит своевременно заметить проблему и вовремя оказать помощь. Не стоит забывать про элементарные правила цифровой гигиены:

– отключать звук на телефоне (использовать только виброрежим);

– держать телефон «на привязи» (не нужно его носить с собой по квартире);

– осознавать, зачем и почему вы взяли телефон в руки.

---

[1] Терехова Е. Иностранные агенты и предписания для соцсетей. Как в России могут заблокировать Facebook и YouTube. URL: https://strana.ua/news/308726-inostrannye-ahenty-i-novye-pravila-raboty-sotssetej-v-rossii-sut-prinjatykh-zakonov-.html (дата обращения: 26.01.21).

При таком подходе для подрастающего поколения будет приоритетна объективная реальность, а не виртуальная.

Максимально защитить свои персональные данные позволит их минимальное использование в интернет-пространстве. Не оставляйте свои телефонные номера и данные на плохо проверенных сайтах. Ведь добровольно подписывая согласие на обработку персональных данных при заключении различных договоров и получении скидочных карт в торговых сетях, мы создаем предпосылки к их передаче третьим (– десятым) лицам без нашего ведома и совершению при их помощи злонамеренных действий в отношении нас.

Таким образом, цифровые технологии, предоставившие неоспоримые блага современному социуму, также несут и потенциальную угрозу государству, бизнесу, традициям, правам и морали человеческого общества, выступая реальным инструментом в руках преступников. Человечество должно научиться находить компромисс между развитием технологий и разумным ограничением данного процесса. Только такая гармония обеспечит безопасное развитие современного мира.

Жильцова Ю.В.,

кандидат психологических наук, доцент
Академия ФСИН России (г. Рязань)

Кузнецов М.И.,

кандидат педагогических наук, доцент
Академия ФСИН России (г. Рязань)

DOI 10.51980/2021_3_82

Противодействие наркорынкам в сети Интернет (опыт США)

Власти США недавно предприняли массовую нейтрализацию наркодилеров на теневом рынке в интернете. Тем не менее желание покупать наркотики, не выходя из дома, и зарабатывать на их продаже гораздо сильнее, чем страх быть осужденным. Несмотря на закрытие почти десяти сайтов, по-прежнему существует около 30 незаконных интернет-рынков, согласно новостному сайту DarknetLive. На одном из них покупатели могут купить пять граммов героина за 0,021 биткойна (около $170) или десятую грамма крэка за 0,0017 биткойна (около $14)[1]. Это означает, что борьба с наркотиками в Интернете начинает выглядеть, как война с ними в физическом мире – организуются рейды, блокируются сайты, несколько системных

[1] URL: https://www.thesouthafrican.com/news/nigeria-drugs-in (дата обращения: 02.02.2021).