убежища, объясняя свои действия стремлением избежать распространения коронавирусной инфекции.

На наш взгляд, основополагающей задачей видится определение согласованных на межгосударственном уровне пределов внутренней компетенции государства в организации миграционного процесса. Реализация права каждого человека покидать любую страну, включая свою собственную, и возвращаться в свою страну (Всеобщая декларация прав человека, Статья 13, п. 2) стоит в зависимости от характера восприятия национальных интересов государственной властью. Политики государств в данной сфере формируются под влиянием множества факторов, среди которых доминирующими являются интересы обеспечения национальной безопасности, охватывающие самые различные сферы общественной жизнедеятельности, в том числе и миграцию [9].

Таким образом, мы приходим к выводу о том, что международно-правовой статус беженцев несмотря на свою казалось бы достаточно полную регламентацию, нуждается в доработке.

1. Статистика вынужденной миграции // <https://www.unhcr.org/ru/stats/> // (дата обращения 26.10.2021)
2. Прудников А.С., Сазон К.Д. Место и роль статуса беженца в национальных системах убежища стран Содружества независимых государств // Вестник Московского университета МВД России. 2015. №7. С. 228-231.
3. Конвенция о статусе беженцев. Принята 28 июля 1951 года // www.un.org/ru/documents/decl_conv/conventions/refugees.shtml // (дата обращения 26.10.2021).
4. Кудрявцева Л.В. Правовой статус иностранных граждан, осуществляющих трудовую деятельность на территории Российской Федерации // Бюллетень науки и практики. 2018. Т. 4. № 5. С. 559-567.
5. Коновалова Е.А., Ткачук А.С. "Мигрант", "беженец": проблема определения понятий и правового статуса в международном праве. Т. 3 № 5 (21). 2018. С. 847-850.
6. Федеральный закон от 19.02.1993 № 4528-1 (ред. от 22.12.2014) «О беженцах» // Консультант Плюс: Законодательство.
7. Волох Владимир Александрович. Трактовка понятия "беженец" в международном праве // Образование и право. 2016. №11. С. 136-140.
8. Карасёва Л.В. Значение норм международного частного права в регулировании трудовых отношений мигрантов из стран СНГ в Российской Федерации. Автореферат диссертации на соискание ученой степени кандидата юридических наук / Российский государственный социальный институт. Москва, 2007. 30 с.
9. Магомедкеримов З.М. К вопросу о статусе беженцев в международном праве. Материалы международной научно-практической конференции. Конституционно-правовое регулирование общественных отношений: теория, методология, практика. 2018. С. 293-303.

Кузнецова И.С., Редников Д.В.

К вопросу об ответственности за компьютерные преступления в России и иностранных государствах

*ФГБОУ ВО Башкирский государственный университет
(Россия, Уфа)*

doi: 10.18411/trnio-11-2021-247

Аннотация

В статье рассматривается вопрос ответственности за компьютерные преступления в России и иностранных государствах, таких как: США, Великобритания, Германия, Украина.

Ключевые слова: компьютерные преступления, информационная безопасность, наказание, правонарушения, киберпреступления.

Abstract

The article deals with the issue of responsibility for computer crimes in Russia and foreign countries, such as the USA, United Kingdom, Germany, Ukraine.

Keywords: computer crimes, information security, punishment, offenses, cybercrimes.

В настоящее время все сферы жизни общества так или иначе связаны с компьютерными технологиями - операции в банках, походы к врачам, заказы и получения посылок, общение в социальных сетях - продолжать можно долго. Информатизация жизни принесла с собой массу удобств, но к сожалению, и привела к обострению проблемы компьютерных преступлений. Так, по статистике МВД России на июль 2021 - за семь месяцев 2021 года произошло почти 320 тысяч киберпреступлений, что на 16% больше, чем за тот же период в прошлом году [1]. Стоит отметить, что часто такие преступления не фиксируются по тем или иным причинам. Киберпреступления могут быть не обнаружены, иными словами организация или физическое лицо могут не обнаружить произошедший инцидент информационной безопасности. Например, у физического лица могли скомпрометировать логин и пароль от его учетной записи на каком-либо сервисе и пользоваться этим сервисом от его имени, при этом пользователь может даже не знать этого. Говоря о юридических лицах, можно выделить преступления с похищением той или иной информации или же с вирусами-майнерами, которые не обнаружила организация, так злоумышленник будет получать выгоду пользуясь оборудованием (в данном случае компьютерами) юридического лица.

Компьютерные преступления (преступления с использованием компьютера) - любые незаконные, неэтичные действия, затрагивающее автоматизированную обработку данных, передачу данных, несущие вред государству, обществу или отдельному человеку.

В статье мы будем рассматривать ответственность за компьютерные преступления прежде всего уголовную, немного упоминая остальные виды.

В России говоря об уголовной ответственности за киберпреступления мы сразу обращаемся к главе 28 Уголовного Кодекса РФ, ее название «Преступления в сфере компьютерной информации» [2].

Статья 272 УК РФ - Неправомерный доступ к компьютерной информации [2]: один из самых часто встречающихся видов компьютерной преступности. Информация, к которой злоумышленники могут получить доступ может быть государственной, коммерческой, банковской или любой другой из видов охраняемых законом информации. Для защиты информации используются различные программные и аппаратные средства защиты, также если речь идет о предприятиях проводится организационная работа с сотрудниками - тренинги по информационной безопасности и т.д. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации - в зависимости от признаков преступления виновному может быть назначено от штрафа 200000 рублей до лишения свободы до 7-ми лет.

Статья 273 УК РФ - Создание, использование и распространение вредоносных компьютерных программ: по этой статье злоумышленникам вменяется [2] - намеренное (с целью извлечения выгоды) создание вредоносных программ, то есть таких компьютерных продуктов, с помощью которых можно: блокировать, уничтожить, модифицировать, копировать информацию, безопасность которой охраняется, а также нейтрализовать средства защиты компьютерной информации. В зависимости от признаков преступления виновному может быть назначено наказание от штрафа 100000 рублей до лишения свободы до 7-ми лет.

Статья 274 УК РФ - Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей [2]: чаще всего вменяется работникам различных предприятий - должностным лицам, на которых возложены обязанности по содержанию информации и поддерживающей инфраструктуры в безопасности. Виновным грозит наказание от штрафа в 500000 рублей до лишения свободы на срок на 5 лет.

И наконец, самая молодая статья (появилась в 2018 году) УК РФ - Статья 274.1 - Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации [2] - любые неправомерные действия, которые направлены на критическую информационную инфраструктуру Российской Федерации. Данный состав преступления

подразумевает угрозу безопасности государства и населения, расследованием таких дел занимаются сотрудники ФСБ. Виновным грозит до 10 лет лишения свободы.

К таким преступлениям можно отнести взлом программного обеспечения для регулирования авиатранспорта. Например, злоумышленник взламывает программное обеспечение диспетчерского пункта, тем самым существует угроза возникновения крушения авиасредства или причинение другого тяжкого вреда с помощью авиасредства. Также, стоит понимать, что к таким преступлениям можно смело отнести киберпреступления, связанные с энергетикой, здравоохранением, военной промышленностью и иными отраслями, представляющими критическую важность для РФ.

К преступлениям, совершенным с критического информационной инфраструктурой следует относиться с особой важностью, так как, зачастую данные преступления могут принести значимый социальный ущерб целому городу или стране.

Так же в России действует ответственность за киберпреступления по кодексу об административных правонарушениях, например, глава 13 кодекса «Административные правонарушения в области связи и информации».

Проблема компьютерных преступлений актуальна во всем мире, рассмотрим законодательства других стран.

Для примера рассмотрим США, из открытых источников известно, что первый законопроект, который ввел уголовную ответственность за преступления в сфере информационных технологий, был создан в 1977 году. Далее, взяв его за основу, в 1984 году в США был принят закон о мошенничестве и злоупотреблении с использованием компьютеров (Computer Fraud and Abuse Act, CFAA), где подробно рассказывается о составах возможных преступлений и наказании за них. Сейчас в США активно заботятся о кибербезопасности, сроки наказаний зависят от тяжести преступлений и обстоятельств дела и могут достигать 30 лет лишения свободы.

Великобритания. С августа 1990 года действует Акт о компьютерных злоупотреблениях, редакции которого выходят и корректируют законодательство. С 2003 года действует Положение о частной информации и электронной связи, регламентирует рассылку спама компаниями. Уголовные наказания в стране существуют по срокам примерно схожи с российскими.

Германия. В уголовном кодексе страны содержится достаточно много параграфов, посвященных компьютерным преступлениям. Например, компьютерное мошенничество в Германии наказывается лишением свободы на срок до 5 лет или штрафом; противоправное аннулирование, уничтожение данных, приведение их в негодность или изменение - лишением свободы на срок до 2 лет или штрафом. Стоит отметить, что в Германии по многим статьям преследование начинается только если потерпевший пишет заявление.

Украина. Большая часть компьютерных преступлений в стране, согласно статистике, связана с мошенничеством в сфере электронной коммерции. Раздел 16 уголовного кодекса страны, а именно преступления в сфере использования компьютеров или выражаясь юридически электронно-вычислительных машин (компьютеров), систем и компьютерных сетей, схож с главой 28 российского УК упомянутого ранее. Существующие статьи: 361 - Незаконное вмешательство в работу компьютеров - электронно-вычислительных машин, сетевой инфраструктуры - систем и компьютерных сетей, 362- Похищение, присвоение, вымогательство цифровой (компьютерной) информации или завладение ею путем мошенничества или злоупотребления служебным положением, 363-Нарушение правил эксплуатации автоматизированных электронно-вычислительных систем, однако наказания более мягкие, чем в России.

Как мы видим, у каждой страны в законодательстве есть свои плюсы и минусы, но это даже хорошо, поскольку страны получают дополнительный стимул к сотрудничеству, объединяя свои усилия против компьютерных преступлений. И это отлично, потому что компьютерные преступления достаточно часто совершаются злоумышленниками из другой страны, то есть чтобы их поймать необходимо сотрудничество государств.

Не секрет, что все страны отличаются как по своим позициям в вопросах безопасности, так и в реальных ситуациях компьютерной преступности внутри. Однако на различных встречах достигается взаимодействие и разрабатываются такие документы, как Конвенции Совета Европы о киберпреступности (Будапештская конвенция) - самый первый международным договор о преступлениях, совершенных через Интернет и другие компьютерные сети, которые помогают противостоять злоумышленникам и защищать информацию.

1. Число киберпреступлений в России [Электронный ресурс] // TADVISER. Государство. Бизнес. IT. / Режим доступа: URL: <https://www.tadviser.ru/>
2. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 01.07.2021) (с изм. и доп., вступ. в силу с 22.08.2021) [Электронный ресурс] // Справочно - правовая система КотсультантПлюс / Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_10699/
3. Канубриков, В.А., Османов, М.М. Способ совершения преступления как составообразующий признак преступлений в сфере компьютерной информации / В.А. Канубриков, М.М. Османов // Образование и право. - 2021. - № 5. - С. 312-315. - DOI: 10.24412/2076-1503-2021-5-312-315
4. Аббуд, Р.Р. Актуальные вопросы международного права в части преступлений в сфере компьютерной информации / Р.Р. Аббуд // Евразийский юридический журнал. - 2021. - № 2 (153). - С. 43-44. - DOI: 10.46320/2073-4506-2021-2-153-43-44
5. Лантух, Э.В., Ишигеев, В.С., Грибунов, О.П. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации / Э.В. Лантух, В.С. Ишигеев, О.П. Грибунов // Всероссийский криминологический журнал. - 2020. - Т. 14. - № 6. - С. 882-890. - DOI: 10.17150/2500-4255.2020.14(6).882-890

Куручкин В.В.

Защита прав пользователей земельных участков сельскохозяйственного назначения

ФГБОУ ВО «Кубанский государственный аграрный университет им. И.Т.Трубилина»
(Россия, Краснодар)

doi: 10.18411/trnio-11-2021-248

Аннотация

В настоящей статье рассматриваются особенности защиты прав пользователей земельных участков сельскохозяйственного назначения; определены перспективные средства и методы обеспечения прав и интересов законных пользователей в пределах установленных границ правового регулирования.

Ключевые слова: земельный участок, право пользования, защита права, законодательство, обязательство, землепользователи.

Abstract

This article examines the features of protecting the rights of users of agricultural land plots; promising means and methods of ensuring the rights and interests of legitimate users within the established boundaries of legal regulation have been identified.

Keywords: land plot, right to use, protection of rights, legislation, obligation, land users.

Положительная динамика роста цен на товары сельскохозяйственного производства, а также слияние энергетического и продовольственного рынка товарной продукции явились причинами внезапного всплеска интереса к приобретению или продаже сельскохозяйственных угодий. В результате на рынке земли повысился интерес к участкам сельскохозяйственного назначения как источнику (средству) создания сельскохозяйственной продукции и, соответственно, источнику дохода.

Такие земли переходят из рук в руки в результате сделок, часто заключаемых между участниками при незначительном или полном отсутствии участия местных общин, которые зависят от доступа к этим землям для обеспечения своих средств к существованию. В целях