

сети Интернет»; а также предусмотреть административную ответственность за оскорбление, совершенное лицом, замещающим государственную должность либо должность государственной гражданской, в связи с осуществлением своих полномочий (должностных обязанностей)».

Библиографические ссылки

1. Кодекс Республики Беларусь об административных правонарушениях от 6.01.2021 № 91-3: принят Палатой представителей 18.12.2020: одобрен Сов.Респ. 18.12.2020 // Консультант Плюс: Беларусь. [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 01.07.2021) (с изм. и доп., вступ. в силу с 01.09.2021 // Консультант Плюс: РФ. [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

3. Постановление Пленума Верховного Суда Республики Беларусь от 23.12.1999 №15 «О практике рассмотрения судами гражданских дел о защите чести, достоинства и деловой репутации» (в ред. постановлений Пленума Верховного Суда от 02.06.2011 №3, от 30.03.2017 №3, от 28.09.2017 № 11).

4. Гражданский кодекс Республики Беларусь от 7.12.1998 № 218-3: пр. Палатой представителей 28.10.1998, одоб. Сов. Респ. 19.11.1998 от 05.01.2021 № 95-3 // Консультант Плюс: Беларусь. [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

Басалай Вероника Ивановна

АДМИНИСТРАТИВНАЯ ОТВЕТСТВЕННОСТЬ ЗА НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Белорусский государственный университет, аспирант кафедры конституционного права юридического факультета, veron_bas@mail.ru

Аннотация. В данной статье рассматриваются проблемные вопросы доступа к компьютерной информации: понятие, состав, квалификация. Раскрыты особенности специфики административной ответственности в данной сфере, которые связаны с ее особым субъектным статусом и определяются социальной сущностью профессиональной деятельности.

Ключевые слова: несанкционированный доступ; неправомерный доступ; информация; компьютерная информация; уголовная ответственность; административная ответственность.

Со вступлением в законную силу нового кодекса Республики Беларусь об административных правонарушениях нормативно-правовая регламентация различных аспектов административного регулирования подвергается существенному обновлению и совершенствованию. Учитывая стремительное формирование информационного пространства, вопросы доступа к компьютерной информации становятся все более актуальными и востребованными. Специфика административной ответственности в этой сфере связана с ее особым субъектным статусом и определяется социальной сущностью профессиональной деятельности.

Кодекс об административных правонарушениях в статье 23.4, как и статья 349 Уголовного кодекса Республики Беларусь предусматривает ответственность за несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты.

Непосредственным объектом правонарушения и преступления за несанкционированный доступ к компьютерной информации является информационная безопасность – совокупность общественных отношений, обеспечивающих состояние защищенности интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Объективная сторона, как в уголовном законодательстве, так и в административном, характеризуется действием, которое выражается в несанкционированном доступе к информации. Под доступом к компьютерной информации следует понимать возможность получения информации и пользования ею. Доступ может осуществляться как непосредственно через информационную компьютерную систему, так и удаленно через другие информационные компьютерные системы посредством использования различных информационных сетей. Сфера регулирования защиты компьютерной информации на законодательном уровне подлежит постоянному совершенствованию. Так, к примеру, можно выделить: Соглашение о порядке защиты конфиденциальной информации и ответственности за ее разглашение при осуществлении Евразийской экономической комиссией полномочий по контролю за соблюдением единых правил конкуренции, подписанное в г. Москве 12 ноября 2014 года; Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий» (заключено в г. Душанбе 28.09.2018); Решение о стратегии обеспечения информационной безопасности государств – участников СНГ (Принято в г. Москве 25.10.2019).

Под информацией как таковой в соответствии со ст. 1 Закона Республики Беларусь от 10.11.2008 № 455-3 «Об информации, инфор-

матизации и защите информации» понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Система защиты информации – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации. Нарушение систем защиты информации (способ совершения правонарушения или преступления), в свою очередь, является обязательным признаком объективной стороны несанкционированного доступа к компьютерной информации.

Статья 1 Конвенции Совета Европы о преступности в сфере компьютерной информации ETS №185 от 23.11.2001 (г. Будапешт) определяет «преступления в киберпространстве как группу преступлений, направленных против конфиденциальности, целостности и доступности компьютерных данных и систем». Так, согласно ст. 2-6 Конвенции к таким преступлениям относятся: 1) незаконный доступ (ст. 2), 2) незаконный перехват (ст. 3), 3) воздействие на компьютерные данные (противоправное преднамеренное повреждение, удаление, ухудшение качества, изменение и блокирование компьютерных данных (ст. 4) или системы (ст. 5), противозаконное использование специальных технических устройств (ст. 6) компьютерных программ, разработанных или адаптированных для компьютерных преступлений, предусмотренных в ст. 2-5, а также компьютерных паролей, кодов доступа, их аналогов, посредством которых может быть получен доступ компьютерной системе в целом или любой ее части.

Определение понятия доступа в научной литературе, по сути, схожи с нормативными. Например, И.А. Клепицкий понимает под доступом к компьютерной информации приобретение и использование лицом возможности получать, вводить, изменять или уничтожать информацию либо влиять на процесс обработки. На основании анализа нормативных и литературных источников можно выделить две существующие позиции относительно содержания понятия «доступ к информации»: 1) только полномочие на ознакомление с информацией; 2) полномочие на ознакомление и использование информации. Представляется, что доступ к информации – комплексное понятие, включающее в себя оба правомочия. Ознакомление, как правило, предполагает возможность дальнейшего использования информации, соответственно, прежде чем воспользоваться информацией, нужно сначала с ней ознакомиться. Возможность ознакомления с информацией без использования ее не представляет общественной опасности – информация должна быть воспринята.

Если обратиться к УК государств – участников СНГ, то можно заметить, что в России, Туркменистане, Азербайджане, Казахстане и Таджикистане такой доступ к информации именуется неправомерным, а в Беларуси, Узбекистане и Армении – несанкционированным. Н.Ф. Ахраменка считает предпочтительным использование прилагательного «неправомерный», которое характеризует сущностный, а не организационный признак доступа. М.Ю. Демьянович полагает, что доступ к компьютерной информации возможен только при наличии определенных законных полномочий, т. е. правового основания, поэтому правильно называть его неправомерным. Описание деяния «неправомерный», «несанкционированный доступ» к компьютерной информации указывает на то, что деяние осуществляется вопреки воле владельца информационного актива, угрожает не только конфиденциальности, но и целостности или доступности.

К примеру, диспозиция статьи 278 УК Республики Узбекистан не содержит указания на то, что компьютерная информация, к которой осуществляется неправомерный доступ, должна быть охраняемой законом, а статья 227 УК Республики Казахстан – содержит термин «охраняемой законом» компьютерной информации.

Полагаем, что специальное указание «охраняемой законом» представляется излишним, а термин «несанкционированный доступ», указывающий на полное отсутствие возможности ознакомления с информацией и отсутствие специального разрешения является предпочтительным.

Что касается субъективной стороны несанкционированного доступа к компьютерной информации, то в уголовном законодательстве (ч. 1 ст. 349 Уголовного кодекса Республики Беларусь) она характеризуется неосторожностью. Субъективная сторона несанкционированного доступа к компьютерной информации в административном праве, в свою очередь, характеризуется как неосторожной, так и умышленной формой вины.

Субъект правонарушения и преступления за несанкционированный доступ к компьютерной информации в уголовном и административном законодательстве также одинаковый – общий, то есть лицо, достигшее 16-летнего возраста.

Представляется целесообразным разграничение ответственности, к примеру, от формы вины субъекта и характера наступления последствий, а также разделение ответственности за неправомерный доступ в зависимости от психического отношения субъекта к наступлению общественно опасных последствий; дифференциацию ответственности в зависимости от наступления последствий.

На основании изложенного, приходим к следующим выводам: 1) доступ к компьютерной информации – комплексное понятие, под которым следует понимать возможность получать, вводить, изменять или уничтожать информацию либо влиять на процесс обработки и пользования ею; 2) термин «несанкционированный доступ» более предпочтительный нежели «неправомерный»; 3) целесообразность разграничения ответственности от формы вины субъекта правонарушения за несанкционированный доступ к компьютерной информации и характера наступления последствий, а также разделение ответственности за неправомерный доступ в зависимости от психического отношения субъекта к наступлению общественно опасных последствий.

Библиографические ссылки

1. Кодекс Республики Беларусь об административных правонарушениях от 06.01.2021 № 91-3: пр. Палатой представителей 18.12.2020: одоб. Сов. Республики 18.12.2020// Консультант Плюс: Беларусь. [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр прав. информ. Респ. Беларусь. – Минск, 2021.
2. Уголовный кодекс Республики Беларусь от 09.07.1999 № 275-3: принят Палатой представителей 02.06.1999: одоб. Сов. Республики 24.06.1999// Консультант Плюс: Беларусь. [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр прав. информ. Респ. Беларусь. – Минск, 2021.
3. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изм. и доп. по сост. на 02.07.2021)/ [Электронный ресурс] – Режим доступа [/https://online.zakon.kz](https://online.zakon.kz). – Дата доступа: 27.09.2021.
4. Уголовный кодекс Республики Узбекистан (утвержден Законом Республики Узбекистан от 22.09.1994 №2012-ХП) (с изм. и доп. по состоянию на 25.08.2021)/ [Электронный ресурс] – Режим доступа <https://online.zakon.kz>. [Электронный ресурс] – Дата доступа: 27.09.2021.

Бічун Вераніка Мечыславаўна

КАНСТЫТУЦЫЙНАЕ ПРАВА РЭЧЫ ПАСПАЛІТАЙ ПЕРЫЯДУ ДЗЯРЖАЎНА-ПРАВАВЫХ РЭФОРМ (ДРУГАЯ ПАЛОВА XVIII ст.)

Беларускі дзяржаўны ўніверсітэт, выкладчык кафедры тэорыі і гісторыі дзяржавы і права юрыдычнага факультэта, bichun.veronika@mail.ru

Анатацыя. Паслабленне каралеўскай улады, бяссілле сойма, саслабелы, архаічны дзяржаўны адміністрацыйны апарат, з аднаго боку, а з другога – узмацненне ўлады магнатаў і ўзмацненне дэцэнтралізацыі дзяржаўнай улады, з’явіліся перадумовамі для абвастрэння з сярэдзіны XVIII ст. унутрыпалітычнай барацьбы ў Рэчы Паспалітай і ўзмацнення патрабаванняў неадкладных рэформаў. У артыкуле разглядаецца