4. Общая рекомендация 19: Насилие в отношении женщин [Электронный ресурс] // UN Treaty Body Database. – Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/cedaw_handbook/cedaw_rec19.pdf. – Дата доступа: 22.11.2021.

5. Пекинская декларация и Платформа Действий [Электронный ресурс] // Организация Объединенных Наций. – Режим доступа: https://www.un.org/womenwatch/daw/beijing/pdf/BDPfA%20R.pdf. – Дата доступа: 22.11.2021.

6. Политическая декларация по ВИЧ и СПИДу: ускоренными темпами к активизации борьбы с ВИЧ и прекращению эпидемии СПИДа к 2030 году [Электронный ресурс] // Организация Объединённых Наций. – Режим доступа: https://undocs.org/ru/A/RES/70/266. – Дата доступа: 22.11.2021.

7. General recommendation № 15: Avoidance of discrimination against women in national strategies for the prevention and control of acquired immunodeficiency syndrome (AIDS) [Electronic resource] // UN Treaty Body Database. – Mode of access: https://tbinternet.ohchr.org/Treaties/CEDAW /Shared%20Documents/1_Global/INT_CEDAW_GEC_4726_E.pdf. – Date of access: 22.11.2021.

В.В. Генюш
ГрГУ им. Янки Купалы (Гродно)

СОСТАВЛЯЮЩИЕ ЭЛЕМЕНТЫ ПОНЯТИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ КАК ОБЪЕКТА УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ

При характеристике преступлений в информационной сфере можно столкнуться с понятиями «кибербезопасность», «цифровая безопасность», которые, как утверждает Д. Г. Полещук, являются синонимами к термину «компьютерная безопасность» [4, с. 14]. О. И. Семыкина и Р. Н. Ключко подчеркивают, что обеспечение охраны от общественно опасных деяний в информационной сфере включает в себя механизм обеспечения кибербезопасности как части информационной безопасности [5, с. 34]. Данную точку зрения разделяют авторы Г. А. Василевич, М. А. Дубко, Д. Г. Полещук, И. Л. Бачило, В. В. Лосев и единогласно отмечают, что кибербезопасность - составляющий технологический элемент обеспечения информационной безопасности. По нашему мнению, компьютерная безопасность справедливо является одним из объектов уголовно-правовой охраны, поскольку, гарантируя компьютерную безопасность, мы защищаем информационную безопасность личности, общества и государства в условиях развития постиндустриального общества. Возникает логичный вопрос: а безопасность каких элементов обеспечивает компьютерную безопасность?

В соответствии с Концепцией информационной безопасности Республики Беларусь, утверждённой постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1, кибербезопасность определяется как «состояние защищённости информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз». На основании данного определения, можем сделать вывод о том, что составляющими элементами компьютерной безопасности являются: 1)

безопасность компьютерной информации, 2) надёжность компьютерной системы, где хранится эта информация.

Первой стороной компьютерной информации является безопасность компьютерной информации. В ч. 18 статьи 4 Уголовного Кодекса Республики Беларусь (далее – УК) содержится определение компьютерной информации, которая толкуется как «информация, хранящаяся в компьютерной системе, сети или на машинных носителях, обрабатываемая компьютерной системой либо передаваемая в пространстве с помощью любых программно-технических средств»[6]. Как верно отмечает И. Л. Бачило, «информация структурируется по целям, интересам, потребностям общества, государства, человека. И это определяет ее особенности как составляющей безопасности во всех других ее сегментах» [1, с. 6]. М. А. Дубко не раз упоминал о важности общественных отношений, обеспечивающих состояние защищённости компьютерной информации при ее получении, передаче, обработке, накоплении, хранении, распространении, предоставлении, а также компьютеров, компьютерных систем [3, с. 11]. Критерии безопасности компьютерной информации (конфиденциальность, целостность, подлинность, доступность и сохранность), которые выделяет автор, напрямую связаны с принятием мер, направленных на защиту данной информации. По нашему мнению, безопасность компьютерной информации предполагает комплекс следующих мер: 1) защита от уничтожения или утраты информации ввиду несанкционированных действий, 2) гарантия недоступности и закрытости данных для любых неавторизованных субъектов системы, 3) обеспечение беспрепятственного доступа к информации и закономерному ее использованию обладателем или уполномоченными лицами, 4) охрана компьютерной информации от неправомерного завладения.

Важно упомянуть, что белорусский законодатель охраняет любую компьютерную информацию. Так, в диспозиции статьи 349 УК предметом несанкционированного доступа выступает компьютерная информация независимо от ее статуса. В то же время российский законодатель в статье 272 УК Российской Федерации указывает, что предметом преступления является только охраняемая законом компьютерная информация, то есть исключительно конфиденциальная информация [7]. Мы поддерживаем позицию защиты компьютерной информации вне зависимости от её статуса, так как одинаковая информация для разных субъектов, в определённых условиях может представлять неодинаковую значимость. Более того, игнорирование защиты несекретных данных может привести к изменению или уничтожению секретных.

Второй стороной компьютерной безопасности является безопасность функций компьютерных систем. Она определяется безотказностью технических средств обработки, хранения, передачи и представления информации, отсутствием сбоев в работе программного обеспечения, целостностью и корректной работой программного обеспечения [2, с. 10].

Следует упомянуть, что компьютерная безопасность достигается за счёт обеспечения двух составляющих одновременно. Как бы ни была доступна, конфиденциальна и целостна компьютерная информация, без целостности программного обеспечения компьютерной системы не обойтись. И наоборот, исключение сбоев в работе компьютерной системы не даёт гарантий безопасности компьютерной информации, которая на ней находится. Таким образом, составляющие

компьютерной безопасности являются взаимозависимыми и не могут существовать отдельно.

Сегодня в Республике Беларусь состояние защищённости компьютерной информации и компьютерных систем как элементов компьютерной безопасности гарантируется нормами уголовного (например, глава 31 УК) и административного (ст. 23.4, ст. 23.5, ст. 23.7, ст. 23.9 Кодекса об административных правонарушениях Республики Беларусь) законодательства. Также в Беларуси вводятся правовые режимы безопасности информации и информационных ресурсов, технические условия политики безопасности, осуществляется выявление и привлечение к установленной законом ответственности лиц, наносящих вред государственным информационным системам, обеспечивается государственная защита интересов граждан и организаций вне зависимости от форм собственности.

Таким образом, безопасность компьютерной информации и безопасность компьютерных систем, где хранится эта информация – составляющие элементы понятия компьютерной безопасности как объекта уголовно-правовой охраны. Для обеспечения кибербезопасности необходимо и дальше осуществлять правовое обеспечение в части выявления информационных угроз, определения степени их общественной опасности и критериев криминализации, которая должна быть своевременной и отвечать духу уголовного закона и принципам иных отраслей права.

Список литературы

1. Бачило, И. Л. Понятийный аппарат информационного права и система обеспечения информационной безопасности / И. Л. Бачило // Труды Института государства и права РАН. – 2016. – № 3. – С. 5–16.

2. Гайдамакин, Н. А. Теоретические основы компьютерной безопасности: учебное пособие / Н. А. Гайдамакин; государственное образовательное учреждение высшего профессионального образования «Уральский государственный университет им. А.М. Горького». – Екатеринбург, 2008.

3. Дубко, М. А. Неправомерное завладение компьютерной информацией как преступление против информационной безопасности: автореф. дис. … канд. юрид. наук : 12.00.08 / М. А. Дубко; Белорус. гос. ун-т. – Минск, 2018. – 26 с.

4. Полещук, Д. Г. Уголовно-правовая охрана информационной безопасности (на примере отдельных аспектов охраны кибербезопасности и защиты информации ограниченного распространения): автореф. дис. ... канд. юрид. наук : 12.00.08 / Д. Г. Полещук ; Белорус. гос. ун-т. – Минск, 2020. – 32 с.

5. Семыкина, О. И. «Цифровой» признак совершения преступлений как вектор криминализации (компаративный обзор подходов государств — участников СНГ) / О. И. Семыкина, Р. Н. Ключко // Журнал зарубежного законодательства и сравнительного правоведения = Journal of Foreign Legislation and Comparative Law. – 2020. – № 6. – С. 34-52.

6. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : принят Палатой представителей 2 июня 1999 г. ; одобр. Советом Респ. 24 июня 1999 г. : изм. и доп. по сост. на 17 нояб. 2021 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. — Минск, 2021.

7. Уголовный кодекс Российской Федерации [Электронный ресурс]: от 13.06.1996 N 63-ФЗ: принят Государственной Думой 24 мая 1996 г. ; одобр. Советом

Федерации 5 июня 1996 г.: изм. и доп. по сост. на 17 нояб. 2021 г.// Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр», Нац. центр правовой информации Республики Беларусь. — Минск, 2021.

А.С. Греков
БГЭУ (Минск)

ОСОБЕННОСТИ МЕЖДУНАРОДНОГО АТОМНОГО ПРАВА

В настоящее время международное атомное право – сравнительно молодое, развивающееся направление международного публичного права. С 1945 года в мире начала развивается ядерная энергетика, а в 1956 году был подписан Устав об учреждении Международного агентства по атомной энергии (далее – МАГАТЭ) [1, с. 11].

Возникновение новой сферы общественных отношений обусловило необходимость координации усилий государств по использованию атомной энергии в мирных целях. В настоящее время международно-правовое регулирование отношений в области использования атомной энергии развивается в следующих направлениях: обеспечение ядерной безопасности и радиационной защиты; регламентация ядерного экспорта и транспортировки ядерных веществ; физическая защита ядерных материалов; атомное судоходство; использование ядерных источников энергии в космосе; охрана окружающей среды от радиоактивного загрязнения; ядерное страхование и установление ответственности за ядерный ущерб; помощь в случае ядерной аварии.

Актуальность исследования проблем атомного права обусловлена необходимостью определения места атомного права в системе международного права, а также надлежащего правового регулирования отношений, складывающихся в процессе использования атомной энергетики.

В научной юридической литературе отсутствует единство терминологии, используются различные термины: «атомное» право либо «ядерное» право, «атомная» энергия либо «ядерная» энергия и т.д. В связи с этим возникает вопрос: какой термин является более корректным не только с точки зрения юридической, но и иных наук? Основываясь на научной литературе, считаем, что, когда речь идёт о регулировании использования энергии, выделяемой в результате преобразования атомов, следует говорить об «атомном» праве и «атомной» энергии. В то же время, если речь идёт об энергии, выделяемой в результате преобразования ядер атомов в ходе цепной ядерной реакции, необходимо говорить о «ядерном» праве и «ядерной» энергии [1, с. 14].

На данном этапе развития атомного права есть основания утверждать, что в системе международного права атомное право является самостоятельной отраслью. Такой точки зрения придерживаются и авторы учебника Международное право МГИМО МИД России под редакцией профессора А.Н. Вылегжанина [2, с. 308]. В настоящее время международное атомное право признается в научной литературе как новая отрасль права. Особенность данной отрасли заключается в самой ее сфере регулирования, связанной с повышенной опасностью для общества. В силу физических свойств ядерная энергия несёт в себе врождённые риски для человека и окружающей среды. Яркие тому примеры аварии на Чернобыльской АЭС и АЭС «Фокусима».

Атомное право базируется на международных конвенциях и договорах и