

Интересным представляется такой вид медиации, как административная медиация, которая была закреплена в книге 1 разд. 1 гл. 4 Административного кодекса Франции. Так, административная медиация – это медиация в административно-правовом споре, в котором одним из участников является государственный орган. Идея применения медиации в сфере административного права сложна. На данный момент было проведено небольшое количество исследований, основанных на эмпирическом опыте, в результате которых были выявлены следующие преимущества использования медиации в административном производстве: 1) сокращение финансовых затрат для сторон; 2) сокращение временных затрат; 3) конфиденциальность; 4) взаимовыгодное решение для каждой из сторон; 5) возможность урегулирования спора на основе принципов справедливости, а не только в соответствии со строгими правовыми нормами.

Если изучить требования, предъявляемые к медиаторам в Республике Беларусь, то медиатором может быть физическое лицо, имеющее высшее юридическое или иное высшее образование, прошедшее подготовку в сфере медиации в порядке, устанавливаемом Министерством юстиции Республики Беларусь, либо имеющее опыт работы в качестве примирителя в соответствии с процессуальным законодательством, получившее свидетельство медиатора, выдаваемое Министерством юстиции Республики Беларусь на основании решения Квалификационной комиссии по вопросам медиации. Медиативное соглашение заключается в письменной форме, подписывается сторонами и медиатором и подлежит исполнению на основе принципов добровольности и добросовестности сторон. Последствия неисполнения медиативного соглашения могут быть установлены сторонами в медиативном соглашении.

В Республики Беларусь вопрос применения процедуры медиации в административном процессе является дискуссионным. Так, отсутствие закреплённого перечня дел, по которым может применяться данная форма урегулирования споров, усложняет применение данного института. Полагаем, что институт медиации является показателем высокого уровня правового сознания граждан, а также развитого гражданского общества, поэтому считаем целесообразным расширение использования медиации в административном процессе Республики Беларусь, используя положительные элементы Республики Франция по рассмотренному вопросу.

***Пыж А. С.***

## **КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ**

*Пыж Артем Сергеевич, магистрант 1 курса Белорусского государственного университета, г. Минск, Беларусь, artemonowi4@mail.ru*

*Научный руководитель: канд. юрид. наук, доцент Валюшко-Орса Н. В.*

Информация, как определяющий фактор развития постиндустриального общества, является стратегическим ресурсом государства. Тем самым угрозы, направленные на информационную безопасность государства,

способны нанести значительный ущерб его суверенитету. Концепция информационной безопасности Республики Беларусь (далее – Концепция) определяет информационную безопасность как состояние защищенности интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере. Следовательно, угрозы информационной безопасности представляют собой совокупность действий и факторов, создающих опасность состоянию защищенности интересов личности, общества и государства в информационной сфере.

Среди угроз информационной безопасности Концепция выделяет: кибератаки, киберинциденты, деструктивное информационное воздействие и иные угрозы.

Кибератака и киберинцидент осуществляются с помощью программных и программно-аппаратных средств и направлены на объекты информационной инфраструктуры. Их отличие состоит в том, что кибератака целенаправленно нарушает функционирование объектов информационной инфраструктуры и создает угрозу безопасности обрабатываемой этими объектами информации, а киберинцидент фактически или потенциально угрожает информации.

Деструктивное информационное воздействие целенаправленно влияет на деятельность государственных органов, общество, граждан с целью причинения ущерба национальной безопасности Республики Беларусь.

С точки зрения источников, согласно Концепции, угрозы информационной безопасности можно разделить на внешние и внутренние. К внешним угрозам информационной безопасности можно отнести: деятельность иностранных структур, направленную на нарушение информационного суверенитета Республики Беларусь, дискредитацию ее конституционных основ, вовлечение ее граждан в экстремистскую деятельность; информационные войны; международную киберпреступность и др.

К внутренним угрозам информационной безопасности можно отнести: киберпреступность; преступность, связанную с нарушением неприкосновенности частной жизни, обработки персональных данных и др.

Кроме того, выделяют антропогенные, техногенные и стихийные носители угроз информационной безопасности.

В качестве техногенных носителей угроз выступают: отказ технических средств и сбой программного обеспечения в информационных системах; в качестве антропогенных – противоправная деятельность отдельных лиц и преступных групп, а также преднамеренные действия и ошибки персонала информационной инфраструктуры.

Угрозы информационной безопасности можно классифицировать также с позиции нарушений требований, предъявляемых к защите информации: конфиденциальности, целостности, подлинности, доступности и сохранности. Угроза целостности информации может выражаться в модификации компьютерной информации; угроза доступности – в ее блокировке; угроза сохранности – в ее уничтожении. Угрозой подлинности может выступать манипулирование информацией, искажение компьютерной

информации. Угроза конфиденциальности информации может реализоваться в незаконном распространении информации ограниченного распространения.

В зависимости от категории доступа информации, угрозы могут быть направлены: на общедоступную информацию, непредставление которой может причинить вред правам и законным интересам граждан; на информацию ограниченного распространения (о частной жизни и персональных данных, государственной, коммерческой, служебной и иной тайны). Кроме того, информация, распространение которой запрещено (пропаганда войны, экстремистской деятельности, порнографии, насилия и жестокости и др.) сама может выступать в качестве угрозы конституционным правам и свободам граждан, духовной жизни общества, интересам государства.

Предложенная классификация, по нашему мнению, может служить основой для оценки угроз информационной безопасности в сфере государственного управления, а также определения мер для их предупреждения, выявления, своевременного пресечения и восстановления нарушенных прав и охраняемых законом интересов субъектов.