Шамаев Владимир Евгеньевич
магистрант
ФГБОУ ВО «Кубанский государственный
аграрный университет им. И.Т. Трубилина»
г. Краснодар, Краснодарский край

К ВОПРОСУ ОБ АКТУАЛЬНЫХ ПРОБЛЕМАХ ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ

Аннотация*: в статье рассмотрены актуальные проблемы защиты государственной тайны. Автор отмечает, что система защиты сведений, отнесенных к государственной тайне, и их носителей формируется из органов защиты государственной тайны, средств и способов защиты государственной тайны, проводимых событий.*

Ключевые слова*: государственная тайна, актуальные проблемы, защита.*

Нынешний период становления российской государственности связан с постоянным реформированием деятельности правоохранительной системы в целом и каждого его составляющего органа в целях улучшения законодательства, регулирующего все сферы социальной жизни, для максимального обеспечения защиты как государственных, так и частных интересов. Вопросы, связанные с государственной тайной, ее охраной, а также проблемы разглашения государственной тайны были актуальны во все времена. Российская Федерация расходует большие бюджетные средства на обеспечение и защиту своей безопасности.

В соответствии с законом РФ от 21.07.1993 N 5485–1 «О государственной тайне», государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Наиболее часто применяемая норма УК РФ – ст. 283 («Разглашение государственной тайны»). В соответствии с Федеральным законом от 12.11.2012 N 190-ФЗ диспозиция ст. 283 УК РФ претерпела изменения в части расширения оснований поступления

сведений, составляющих государственную тайну, к виновному, а именно в абз. 1 ч. 1 ст. 283 слова «или работе» были замены словами «работе, учебе или в иных случаях, предусмотренных законодательством Российской Федерации», этим же Законом в гл. 19 УК РФ была введена новая ст. 283.1 «Незаконное получение сведений, составляющих государственную тайну». Необходимость подобных изменений авторы законопроекта мотивировали тем, что имеют место случаи, когда иностранный гражданин в силу возложенных на него обязанностей становится обладателем сведений, составляющих государственную тайну, на законных основаниях. При данном анализе ст. 283 УК РФ, предусматривающей ответственность за разглашение государственной тайны, показывает, что субъектом данного действия или бездействия может быть лишь только гражданин Российской Федерации. Следовательно, разглашение иностранным гражданином, допущенным к сведениям, составляющим государственную тайну, указанных сведений в настоящее время не относится к числу уголовно наказуемых деяний. Введение в УК РФ нормы, устанавливающей ответственность за незаконное получение сведений, составляющих государственную тайну, лицом, которому она не была доверена или не стала известна по службе или работе, при отсутствии признаков государственной измены или шпионажа, позволит обеспечить системность охраны различных видов информации ограниченного доступа (например, коммерческой, банковской и государственной тайны) и будет способствовать повышению эффективности защиты государственной тайны от общественно опасных посягательств со стороны лиц, не являющихся ее законными обладателями.

Защита информации делится на решение двух основных групп задач: своевременное и абсолютное удовлетворение информационных потребностей, образующихся в процессе управленческой, инженерно-технической, рекламной и другой деятельности, т. е. обеспечение специалистов организаций, предприятий и фирм секретной или конфиденциальной информацией; ограждение засекреченной информации от несанкционированного доступа к ней конкурента, иных субъектов в злостных целях.

При решении первой группы задач предусматривается, собственно что специалисты имеют все шансы применить как открытую, так и например засекреченную информацию. Снабжение специалистов открытой информацией ничем не ограничивается, не считая ее фактического присутствия. При снабжении же специалиста засекреченной информацией действуют ограничения: присутствие соответствующего допуска (к какой степени секретности информации он допущен) и разрешения на доступ к определенной информации.

Вторая группа задач – ограждение защищаемой информации от несанкционированного доступа к ней конкурента. Она включает такие обстоятельства, как: оборона информационного суверенитета государства и расширение возможностей страны по укреплению собственного могущества за счет формирования и управления развитием своего информационного потенциала; создание критерий эффективного применения информационных ресурсов общества; обеспечение безопасности защищаемой информации: предотвращение хищения, утраты, несанкционированного уничтожения, модификации, блокирования информации и т. п., вмешательства в информацию и информационные системы; сохранение секретности информации в соответствии с установленными правилами ее защиты, в том числе предупреждение ее утечки и несанкционированного доступа к ее носителям; сохранение полноты, достоверности, целостности информации и ее массивов и программ обработки; недопущение безнаказанного растаскивания и нелегального использования интеллектуальной собственности, принадлежащей государству. При рассмотрении проблем защиты информации часто затрагивается вопрос о режиме секретности или конфиденциальности (в последующем – режим секретности). Режим секретности считается частью системы обороны засекреченной информации, а вернее, это осуществление системы защиты информации для определенного объекта или одного из его структурных подразделений или определенной работы. Ведущее предназначение режима секретности – гарантировать соответствующий уровень защиты информации, так как чем выше степень ее секретности, тем больше возрастает уровень ее защиты устанавливается, соответственно и меняется режим секретности. Режим

секретности – это не регламентация правовых норм и правил защиты сведений, а осуществление на определенном объекте действующих норм и правил защиты сведении, составляющих государственную тайну, установленных и регламентированных надлежащими законодательными и подзаконными нормативными актами. Режим секретности включает следующие главные группы мер: для начала, разрешительную систему, определяющую порядок доступа в служебных целях конкретных сотрудников к определенной защищаемой информации и в конкретные помещения, где проводятся скрытые или секретные работы; затем, порядок и критерии делопроизводства с секретными или конфиденциальными документами и другими носителями защищаемой информации. Вполне вероятно деление потоков документальной информации по степени секретности сведений, содержащихся в документах, а также разделение потоков информации, документов, содержащих государственную и коммерческую тайну; в-третьих, установление пропускного и внутриобъектового режима, соответствующего степени секретности информации, имеющейся на объекте; в-четвертых, воспитательно-профилактическую работу, уровень и оглавление которой должны соответствовать уровню требуемой защиты информации с целью предупредить или очень уменьшить риск утечки засекреченной информации через сотрудников объекта, работающих с подобной информацией.

В ст. 2 Закона РФ «О государственной тайне» дано определение системы защиты этой тайны: «Под системой защиты государственной тайны понимается совокупность органов защиты государственной тайны, используемых ими средств и способов защиты сведений, составляющих государственную тайну, и их носителей, а также событий, проводимых в данных целях».

Можно сказать, система защиты сведений, отнесенных к государственной тайне, и их носителей формируется: из органов защиты государственной тайны; средств и способов защиты государственной тайны; проводимых событий.