|  |  |
| --- | --- |
| **УДК 338.486.1.025.3** | |
|  | **Е.А. Шумаева,** *к. гос. упр., доц.,*  **Г.С. Джура**  *Донецкий национальный технический университет,*  *Донецк, Донецкая Народная Республика*  ***E.A. Shumaeva, G.S. Dzhura***  *Donetsk national technical University,*  *Donetsk, Donetsk People's Republic* |
|  |  |
| ПРОБЛЕМЫ ЛИЦЕНЗИРОВАНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ | |
|  | |
| **PROBLEMS OF LICENSING IN THE SPHERE OF INFORMATION SECURITY IN THE RUSSIAN FEDERATION** | |

*Аннотация. В статье исследованы проблемы лицензирования сферы информационной безопасности в Российской Федерации. Проанализированы актуальные вопросы обеспечения информационной безопасности в РФ. Выявлены актуальные проблемы обеспечения лицензирования критической информационной инфраструктуры РФ.*

*Ключевые слова: лицензирование, сертификация, информационная безопасность критическая информационная инфраструктура, техническая защита информации.*

*Abstract. The article investigates the problems of licensing the sphere of information security in the Russian Federation. The topical issues of information security in the Russian Federation are analyzed. The actual problems of licensing of critical information infrastructure of the Russian Federation are revealed.*

*Keywords: licensing, certification, information security critical information infrastructure, technical protection of information.*

**Постановка проблемы.** Рост охвата и развития технологий во всех сферах деятельности государства и общества, обуславливает необходимость обеспечения безопасности государственных информационных ресурсов как стратегическую и краеугольную задачу любого современного государства. Важность обеспечения безопасности информации сегодня очевидна для большинства отраслей и сфер деятельности.

На сегодняшний день, когда современные информационные технологии интенсивно внедряются во все сферы жизни и деятельности общества, национальная, и, как ее часть, экономическая безопасность государства начинает напрямую зависеть от обеспечения информационной безопасности. Именно поэтому с целью создания гарантий по обеспечению необходимой надежности средств защиты информации государство берет на себя ответственность за лицензирование деятельности организаций, занимающихся защитой информации и сертификацию соответствующих технических средств.

Законодательные и административные меры для регулирования вопросов защиты информации на государственном уровне применяются в большинстве развитых стран мира. Компьютерные преступления приобрели в странах с развитой информационно-телекоммуникационной инфраструктурой такое широкое распространение, что для борьбы с ними в уголовном законодательстве предусмотрены различные виды ответственности.

**Анализ последних исследований и публикаций.** В ходе исследования проблем лицензирования в сфере информационной безопасности в Российской Федерации были изучены работы таких авторов, как Лунин Е.И., Атаманов А.Н., Соловьев А.И., Демидов А.А, Терещенко Л.К., Багдасарян В.Э., Афанасьев А.В., Бакравкин С.Г. и др.

**Цель статьи** – проанализировать проблемы лицензирования в сфере информационной безопасности.

**Основные результаты исследования.** Термин «информационная безопасность» в разных контекстах имеет различный смысл. К примеру, в Доктрине информационной безопасности РФ вышеупомянутый термин используется в широком смысле и подразумевает под собой состояние защищенности национальных интересов в информационной сфере, определяемых сбалансированной совокупностью интересов личности, общества и государства.

В Федеральном Законе Российской Федерации «Об участии в международном информационном обмене» термин «информационная безопасность» определяется как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций и государства.

Однако, по мнению авторов, объекту исследования наиболее применим более узкий термин, определяющий термин «информационная безопасность» как защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Стоит отметить, что законодательство Российской Федерации определяет защиту информации, как принятие правовых, организационных и технических мер, направленных на выполнение следующих условий:

– обеспечение защиты информации от несанкционированного доступа (НСД), уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении информации;

– соблюдение конфиденциальности информации с ограниченным доступом;

– реализация права на доступ к информации.

Функционирование государственной системы обеспечения информационной безопасности предполагает наличие соответствующей информационной инфраструктуры, которая представлена в виде аппаратного и программного обеспечения, сетей связи, процессов и объектов, необходимых для функционирования вышеперечисленных компонентов, а также неотъемлемым компонентом являются человеческие ресурсы.

Обеспечение безопасности критической информационной инфраструктуры (КИИ) является одним из важнейших условий удовлетворения законных прав и интересов граждан любой страны, устойчивого функционирования наиболее важных сфер жизнедеятельности современного общества, обороноспособности страны и в целом безопасности государства.

Понятие «КИИ» в Российской Федерации раскрывается как «совокупность автоматизированных информационных систем управления производственными и технологическими процессами (АСУ) критически важных объектов инфраструктуры (КВО) Российской Федерации и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей (ИКС), предназначенных для решения задач управления государством, обеспечения обороноспособности, безопасности и правопорядка, нарушение (либо прекращение) функционирования которых может стать причиной наступления тяжких последствий» [2].

Стоит отметить, что реализация положений государственной политики в области обеспечения информационной безопасности КИИ требует дальнейшего всестороннего развития правовых и организационных принципов и норм, регулирующих соответствующие общественные отношения, т.е. национальную составляющую правового обеспечения безопасности КИИ.

В этой связи приоритетного внимания заслуживают следующие проблемы:

– установление порядка лицензирование (разрешительного порядка) деятельности в области обеспечения безопасности АСУ и КВО информационно-телекоммуникационных сетей;

– развитие системы сертификации как программных, так и аппаратных, составляющих информационных систем КИИ;

– организация взаимодействия субъектов обеспечения безопасности КИИ в рамках государственной системы обнаружения и предупреждения компьютерных атак на объектах КИИ;

– расширение участия государства и организаций в оперативном управлении сетями связи общего пользования в целях минимизации ущерба от кибератак на ИКС КИИ.

Сегодня установление порядка лицензирования деятельности в области обеспечения безопасности АСУ КВО и ИКС требует также и развития отраслевого законодательства. Законодательством в области связи, к примеру, установлено, что деятельность индивидуальных предпринимателей и юридических лиц по оказанию услуг связи, с использованием сетей электросвязи, в том числе применяемых в ИКС, осуществляется только на основании лицензии. Также предусмотрена возможность предъявления требований к сетям связи по построению, управлению или нумерации, применяемым средствам связи, организационно-техническому обеспечению устойчивого функционирования сетей связи, в том числе в чрезвычайных ситуациях, защиты сетей связи от НСД и передаваемой с помощью них информации.

С данной точки зрения для выполнения положений государственной политики содержание лицензий в том числе по оказанию операторами сетей связи общего пользования услуг связи, связанных с обеспечением функционирования ИКС для решения задач государственного управления, обеспечения обороноспособности, правопорядка и безопасности, может быть расширено.

Стоит отметить, что на сегодняшний день в меньшей степени урегулированы правоотношения в области лицензирования деятельности субъектов обеспечения безопасности АСУ КВО. В настоящее время лицензирование деятельности в области обеспечения безопасности КВО не используется в полном масштабе.

Так, в процессе использования атомной энергии предусмотрена выдача органами государственного регулирования в сфере обеспечения безопасности эксплуатирующим организациям, а также организациям, выполняющим работы и предоставляющим услуги в данной области, разрешения (лицензии) на право ведения соответствующих работ, в том числе в сфере обеспечения промышленной безопасности.

Стоит отметить, что создание системы лицензирования деятельности в сфере обеспечения информационной безопасности АСУ КВО требует введения существенных правовых нововведений. Необходимо будет установить порядок предоставления лицензии, определения срока ее действия, отказа в выдаче лицензии, ее переоформления, внесения дополнений и изменений, возобновления и приостановления деятельности, аннулирования лицензии, а также формирования и ведения реестра лицензий.

Сертификация устройств и систем, входящих в состав АСУ КВО и ИКС, рассматривается в качестве важнейшего средства снижения уровня опасности угроз безопасности КИИ. Законодательством РФ в сфере связи для обеспечения, устойчивости функционирования, целостности и безопасности установлено обязательное подтверждение соответствия установленным требованиям средств связи сети общего пользования. Подтверждение соответствия средств связи осуществляется на соответствие техническому регламенту и требованиям, предусмотренным нормативными правовыми актами федерального органа исполнительной власти в области связи. Подтверждение соответствия может быть осуществлено через введение обязательной сертификации либо принятие декларации о соответствии. Для проведения обязательной сертификации средства связи должны предоставляться изготовителем или продавцом.

Сертификация иных средств и устройств ИКС и АСУ КВО в Российской Федерации не предусмотрена. С целью формирования системы сертификации упомянутых систем и устройств необходимо определение признаков и критериев их отнесения к АСУ КВО и ИКС, принятие регламентов и порядков, устанавливающих требования к безопасности использования рассматриваемых средств и устройств, а также создание системы организаций, осуществляющих сертификацию [3].

Цели лицензирования можно условно подразделить на две группы: цели, направленные на защиту личных прав граждан, и цели, направленные на защиту государственных интересов.

К первой группе относятся: предотвращение ущерба правам, законным интересам, жизни или здоровью граждан, окружающей среде, объектам культурного наследия (памятникам истории и культуры), а также народов Российской Федерации.

Вторая группа включает: предотвращение ущерба обороне и безопасности государства, возможность нанесения которого связана с осуществлением индивидуальными предпринимателями и юридическими лицами отдельных видов деятельности.

Указанный перечень целей лицензирования в обобщенном виде является исчерпывающим, а нарушения лицензиатом могут повлечь за собой аннулирование или прекращение действия лицензии, привлечение к ответственности в соответствии с нормами действующего законодательства Российской Федерации, которым установлены основные критерии отнесения отдельных видов деятельности к лицензируемым. Важно учитывать, что только при наличии одновременно всех необходимых критериев вид деятельности может быть признан подлежащим лицензированию.

Рассмотрим основные принципы осуществления лицензирования видов хозяйственной деятельности в Российской Федерации:

– обеспечение единства экономического пространства на территории РФ;

– установление единого порядка лицензирования отдельных видов деятельности на территории РФ;

– установление полноценных перечней лицензионных требований в отношении лицензируемых видов деятельности положениями о лицензировании конкретных видов осуществляемой деятельности;

– установление федеральным законодательством лицензируемых видов деятельности;

– открытость и доступность информации о лицензировании, за исключением информации, распространение которой запрещено или ограничено в соответствии с законодательством;

– соблюдение законности при осуществлении лицензирования [4].

Все перечисленные принципы относятся к основополагающим началам существования института лицензирования и обладают своей спецификой применимо к данной сфере государственной деятельности. Указанные принципы тесно связаны между собой и все вместе создают систему принципов лицензирования, которая отражает сущность правовой природы института лицензирования как федеральной законодательной меры ограничения прав и свобод человека и гражданина в целях защиты здоровья, прав и законных интересов иных лиц, обеспечения обороны и безопасности государства, а также охраны окружающей среды.

Во всем мире сегодня, согласно общепринятым законодательным нормам, большая часть производимой и реализуемой продукции, а также сервисных услуг подлежат сертификации и лицензированию. Однако данные понятия важно четко дифференцировать между собой.

Лицензия – это разрешение на осуществление того или иного вида деятельности.

Под лицензированием понимают комплекс мероприятий, направленных на выдачу лицензий, а также прекращение, приостановление, возобновление, аннулирование этих разрешительных документов. Предоставление лицензий в большинстве случаев осуществляется на основании аудита и заключений комиссии, проверяющей персонал компании, оборудование, технологии производства и другое на соответствия действующим правилам, нормам, требованиям и стандартам.

Сертификат – документ, подтверждающий соответствие товара или услуги определенным требованиям, нормам и критериям.

В случае сертификации проверке и исследованиям подвергается непосредственно продукция, однако если сертифицируется производство – то исследуют и технологии, и оборудование, как и при лицензировании.

Под сертификацией понимают подтверждение соответствия выпущенной или поставленной на территорию государства продукции стандартам, нормативам, правилам и иным документам [5, 6].

Сегодня необходимо обеспечение гарантий того факта, что используемые средства обеспечения безопасности КИИ способны обеспечивать необходимый уровень защиты активов организаций. Именно такой инструмент как лицензирование может способствовать тому, что вопросом защиты информации будут заниматься только высококвалифицированные специалисты, а создаваемые ими продукты будут находиться на должном уровне в результате чего смогут пройти сертификацию.

Без проведения сертификации не представляется возможным оценить, содержит ли то или иное средство потенциально вредные возможности, наличие которых особенно характерно для большинства зарубежных продуктов, которые способные в определенный момент привести к сбоям в функционировании системы, или отдельных ее компонентов, а в крайних случаях к необратимым для нее последствиям. Ярким примером таких возможностей является заложенная фирмой Ericsson при разработке телефонных станций, на базе которых Министерство транспорта РФ строило телефонную сеть, возможность блокировать работу Министерства при получении вызова определенного телефонного номера, который фирма отказывается назвать, и данный пример не является единственным в своем роде.

Сегодня процесс сертификации программного продукта занимает примерно столько же времени, сколько и его разработка, и практически невозможен без исходных текстов программ с комментариями. В то же время известно множество примеров, когда зарубежные фирмы не желали представлять исходные коды своих программных продуктов в российские сертификационные центры под теми или иными предлогами [7].

Трудности с сертификацией ведут к ситуации, когда сертификат быстрее получат самые простые продукты, вследствие чего они будут казаться пользователю более надежными. Длительные же сроки сертификации приводят к тому, что фирма-разработчик успевает вывести на рынок новую версию своего продукта, и процесс становится бесконечным.

Таким образом, к числу наиболее важных направлений совершенствования правового обеспечения безопасности КИИ можно назвать следующие:

– утверждение разрешительного порядка (лицензирования) деятельности в области обеспечения безопасности ИКС и АСУ КВО;

– взаимодействие субъектов системы обеспечения безопасности КИИ в рамках государственной системы обнаружения и предупреждения компьютерных атак на объектах КИИ;

– организация процесса сертификации устройств и систем, составляющих КИИ;

– участие государства в оперативном управлении сетями связи общего пользования в целях минимизации последствий атак на ИКС КИИ.

Учитывая существующие требования к информационной безопасности в Российской Федерации и мировые практики деятельности в сфере обеспечения информационной безопасности, представляется целесообразным присоединение России к сложившимся системам международной стандартизации и сертификации информационных технологий, что на практике означает:

– приведение национальных и отраслевых стандартов в соответствие с международными;

– участие представителей России в международных системах сертификации (в том числе в сертификационных испытаниях);

– возможность признания в России международных сертификатов.

Кроме того, важно отметить, что в соответствии с действующим законодательством Российской Федерации, любая организация, занимающаяся сбором и обработкой персональных данных (к примеру, операций с пластиковыми картами, либо выдачей займов), должна иметь лицензию на право заниматься подобной деятельностью и использовать для этого только сертифицированные средства обеспечения информационной безопасности.

**Выводы.** Ввиду интенсивного перехода всех родов взаимодействий государственного уровня на инфокоммуникационную платформу, задача обеспечения безопасности информации приобретает общегосударственный масштаб.

Мировой опыт совершенствования государственного управления подтверждает, что информационно-аналитическое обеспечение можно рассматривать только как одно из стратегических и краеугольных направлений повышения эффективности деятельности государства, а защита государственных информационных систем и активов должна рассматриваться как стратегический вопрос обеспечения национальной безопасности.

Проблема лицензирования в сфере информационной безопасности на сегодняшний день является крайне актуальной, главным образом потому, что данный инструмент является безальтернативным в разрезе контрольно-надзорной деятельности государства.

|  |  |
| --- | --- |
|  | |
| **Список литературы** | |
|  | Федеральный закон Российской Федерации от 27.07.2006 N 149-ФЗ (ред. от 18.12.2018) «Об информации, информационных технологиях и о защите информации». Статья 16. |
|  | Критическая информационная инфраструктура 2019 год [Электронный ресурс] – Режим доступа: https://rtmtech.ru/articles/kriticheskaya-informatsionnaya-infrastruktura-2019/. |
|  | Проблемы правового обеспечения безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс] – Режим доступа: http://internetinside.ru/problemy-pravovogo-obespecheniya-bezo/. |
|  | Федеральный закон РФ от 04.05.2011 N 99-ФЗ (ред. от 27.12.2018) «О лицензировании отдельных видов деятельности» (с изм. и доп., вступ. в силу с 01.03.2019). Статья 4. |
|  | Сертификация и лицензирование: в чем разница? [Электронный ресурс] – Режим доступа: http://www.lawmos.ru/advice/567/. |
|  | Лицензирование и сертификация [Электронный ресурс] – Режим доступа: https://cs-garant.ru/licenzirovanie\_i\_sertifikacija. |
|  | Лицензирование и сертификация в области защиты информации [Электронный ресурс] – Режим доступа: https://studfiles.net/preview/5852002/page:27/. |