ПРАВОВОЕ ОБОСНОВАНИЕ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

*Шахалов И. Ю.**

The legal basis for the certification of means of information protection

*Igor' Shakhalov **

Аннотация. *Проводится анализ действующих нормативно-правовых актов Российской Федерации, на основании которого определяются случаи, когда сертификация обязательна, с учетом принадлежности информации как к государственному информационному ресурсу, так и к негосударственному информационному ресурсу. Рассматриваются необходимость и обязательность проведения сертификации программных и программно-аппаратных изделий по требованиям информационной безопасности. Делается акцент на сертификацию средств защиты информации при защите информации, как содержащей сведения, составляющие государственную тайну, так и информации, содержащей сведения ограниченного распространения, не содержащие государственную тайну. Приводятся также аргументы об обязательности сертификации с практической точки зрения и обосновывается необходимость проведения аттестации защищаемой информационной системы, что влечет за собой применение сертифицированных средств защиты информации.*

Abstract. *An analysis of the existing normative legal acts of the Russian Federation is carried out, based on which cases are determined when certification is mandatory, considering that information may belong to a government as well a non-government information resource. The need and obligatoriness to carry out the certification of software and hardware-cum-software products for information security are considered. Emphasis is put on the certification of means of information protection while protecting information containing state secrets as well as limited dissemination information that does not contain state secrets. Arguments are also presented on the obligatoriness of certification from a practical standpoint and the need for carrying out an attestation of the information system to be protected which entails using certified means of information protection.*

Ключевые слова: *сертификация, сертификационные испытания, средства защиты информации, информационная безопасность, безопасность программ.*

Keywords: *certification, certification tests, means of information protection, information security, software security.*

Введение

В настоящее время в печати продолжаются дискуссии о необходимости сертификации программно-аппаратных изделий по требованиям безопасности информации [1]. В данной статье мы рассмотрим некоторые правовые вопросы по данной тематике.

Определение понятийного аппарата

Как известно, потребность в сертификации средств защиты информации (СЗИ) по требованиям безопасности информации возникла в связи с появлением частной собственности на СЗИ. Это закономерно привело к тому, что наиболее актуальными стали вопросы защиты государ-

* ***Шахалов Игорь Юрьевич,*** доцент Московского государственного технического университета им. Н. Э. Баумана, заместитель Генерального директора по экспертизам ЗАО «НПО «Эшелон», Российская Федерация, г. Москва.

Shakhalov Igor' Iur'evich, Associate Professor at Bauman Moscow State Technical University, Deputy Director General for Expert Examinations of ZAO [CJSC] "NPO "Eshelon", Russian Federation, Moscow.

E-mail: i.shahalov@npo-echelon.ru

ственной тайны, что послужило одной из причин выхода Федерального закона «О государственной тайне», на базе которого было принято Постановление Правительства РФ № 608 от 26 июня 1995 г. Во исполнение требований ПП РФ № 608 обязательность сертификации СЗИ была закреплена в нормативно-методических документах (НМД) федеральных органов исполнительной власти (ФОИВ), являющихся регуляторами в области защиты информации, а в «Положении о сертификации СЗИ», утвержденном приказом № 199 Председателя Гостехкомиссии России введено понятие аттестации объектов информатизации, как составной части системы сертификации СЗИ [2, 3].

В последующем обязательность сертификации СЗИ при защите информации, содержащей сведения ограниченного распространения, не составляющие государственную тайну (далее «гостайну»), были определены в российском законодательстве, в частности, в постановлении Правительства РФ от 15 мая 2010 г. № 330, в ряде нормативно-правовых актов по защите персональных данных и других.

В 608 постановлении Правительства сказано, что сертификация средств защиты информации осуществляется на основании требований государственных стандартов, нормативных документов, утверждаемых Правительством Российской Федерации и федеральными органами по сертификации в пределах их компетенции.

В свою очередь, НМД ФСТЭК России дает следующее определение сертификации:

Под сертификацией средств защиты информации по требованиям безопасности информации понимается деятельность по подтверждению характеристик средств защиты информации требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных Государственной технической комиссией при Президенте Российской Федерации (Гостехкомиссией России).

Это определение осталось актуальным и после преобразования Гостехкомиссии России в Федеральную службу по техническому и экспортному контролю.

Правовое обоснование обязательности сертификации

При определении обязательности сертификации СЗИ удобно провести классификацию защищаемого информационного ресурса и объектов информатизации [4].

В качестве признаков классификации информационного ресурса выделяют два: принадлежность к государственному информационному ресурсу и уровень ограниченности доступа.

Для защиты государственного информационного ресурса требования устанавливает и контролирует сам собственник (государство). В других случаях, то есть при защите информации, не принадлежащей государству, могут быть неоднозначности, так как требования обязательной сертификации носят, в данном случае, рекомендательный характер [5].

При идентификации уровня ограниченности доступа выделяют:

- государственную тайну,
- персональные данные,
- другие виды тайн, не отнесенные к гостайне и персональным данным,
- открытую общедоступную информацию.

Заметим, что в случае, когда говорят об информации ограниченного доступа, не отнесенной к гостайне, ее исторически часто называют информацией конфиденциального характера или просто конфиденциальной информацией.

Дополнительно могут быть определены требования к системам обработки информации, независимо от классификации обрабатываемой информации.

Назовем основные случаи, когда сертификации СЗИ в нашей стране обязательна (Таблицу 1):

- защищаемая информация составляет сведения, отнесенные к государственной тайне;
- защищаемая информация ограниченного доступа, но не отнесенная к гостайне, при условии, что она относится к государственному информационному ресурсу;
- защищаемая информация относится к персональным [6];
- к защите объектов информатизации (систем, комплексов) определены требования по оценке соответствия независимо от видов тайн.

К примеру, в случае защиты государственной тайны требования по обязательной сертификации СЗИ определены в Законе РФ «О государственной тайне» 1993 г. № 5485-I, Постановлении Правительства РФ 1995 г. № 608 и в других документах.

Требования по сертификации средств защиты информации конфиденциального характера в государственных организациях определены в Постановлении Правительства РФ 2010 г. № 330 (п.6), а также в нормативных документах ФСБ России и ФСТЭК России.

Таблица 1. Основание для требования по сертификации средств защиты информации

Информационный ресурс	Государственная тайна	Персональные данные	Другие тайны	Открытая общедоступная информация
Государственный информационный ресурс	Да	Да	Да	Для систем общего пользования и для специфических систем
Негосударственный информационный ресурс	–	Да	Только для специфических систем	Только для специфических систем

Требования по сертификации средств защиты персональных данных прямо вытекают из Постановления Правительства РФ 2010 г. № 330 (п.6) и косвенно из Постановления Правительства Российской Федерации от 01.11.2012 № 1119 (п.13 г), а также регламентируются нормативными документам ФСБ России и ФСТЭК России.

В остальных случаях необходимо руководствоваться нормативными требованиями к специфическим объектам. Примерами таких объектов являются:

- информационные системы критически важных объектов;
- автоматизированные системы управления технологическим процессом;
- системы управления экологически опасными производствами, объектами, имеющими важное оборонное или экономическое значение и влияющими на безопасность государства;
- федеральные государственные информационные системы общего пользования;
- автоматизированные системы систем вооружений;
- игровые автоматы и др.

С практической точки зрения обязательность сертификации СЗИ диктуется обычно двумя обстоятельствами. Первое связано с требованиями заказчика, который формулирует их к разработке, поставке, внедрению защищенной информационной системы. Например, в техническом задании или техническом проекте на опытно-конструкторскую работу (и дальнейшего авторского надзора или техподдержки) со стороны заказчика было бы правильным указать ГОСТ Р 51583:2000 «Порядок создания автоматизированных систем в защищенном исполнении». Согласно п. 4.15 этого стандарта необходим сертификат соответствия.

Другой случай связан с необходимостью быть уверенным в защищенности объекта с формальной точки зрения, когда требуется заполучить какой-нибудь официальный документ о подтверждении соответствия информационной системы требованиям российского законодательства. В настоящее время в области информационной безопасности таким документом является аттестат соответствия. Никто не выпишет такой аттестат без сертифицированных СЗИ.

В рамках сертификации регламентирован инспекционный контроль [7] и два вида сертификационных испытаний:

- испытания на отсутствие недекларированных возможностей в программном обеспечении средств защиты информации [8-11];
- испытаний по защищенности информации от несанкционированного доступа [4,12].

В настоящее время наблюдается развитие системы сертификации средств защиты информации в направлении применения национального стандарта ГОСТ Р ИСО/МЭК 15408 [13,14]. Первыми нормативно-правовыми актами, отражающими новый подход, стали документы по системам обнаружения вторжений и средствам антивирусной защиты [15,16]. Отдельно следует упомянуть проекты нормативных документов по технологиям безопасной разработки программных средств защиты информации, которые проходят апробацию в рамках деятельности Технического комитета по стандартизации ТК-362 «Защита информации» [17].

В заключение следует заметить, участники сертификации (заявитель, испытательная лаборатория и орган по сертификации) должны

иметь соответствующие лицензии на конкретный вид деятельности [18, 19].

Выводы

Итак, рассмотрев вкратце вопрос об обязательности сертификации средств защиты информации с правовой точки зрения, можно сделать следующий вывод.

Сертификация средств защиты информации обязательна во всех случаях, когда речь идет о защите информации, входящей в государственные информационные ресурсы, то есть когда собственником информации является государство. Это означает, что при формировании технического задания на проекты государственных информационных систем в обязательном порядке указываются требования по сертификации средств защиты информации [20]. Для коммерческих структур с защитой их коммерческих и других тайн, сертификация носит рекомендательный характер, т.е. оценка соответствия систем и средств защиты информации может быть ограничена разного рода аудитом по безопасности информации [21].

Несколько особняком стоит проблема защиты персональных данных – их надо защищать всем и всегда, несмотря на организационно-правовой статус предприятия и его принадлежность, так как собственником персональных данных является не предприятие, а непосредственно сам субъект персональных данных. При этом информационная система персональных данных (ИСПДн) не может пройти полноценную и адекватную оценку соответствия без проведения аттестационных испытаний, которые невозможны без применения в ИСПДн сертифицированных СЗИ [6].

Литература

1. Павел М. Кому нужна сертификация? // Information Security. 2014. № 6. С. 40–41.
2. Костогрызов А.И., Липаев В.В. Сертификация функционирования автоматизированных информационных систем. М.: Изд. «Вооружение. Политика. Конверсия», 1996. 280 с.
3. Марков А., Цирлов В. Сертификация программ: мифы и реальность // Открытые системы. СУБД. 2011. № 6. С. 26–29.
4. Методы оценки несоответствия средств защиты информации / А.С. Марков, В.Л. Цирлов, А.В. Барабанов; под ред. А. С. Маркова. М.: Радио и связь, 2012. 192 с.
5. Марков А.С., Цирлов В.Л., Маслов В.Г., Олексенко И.А. Тестирование и испытания программного обеспечения по требованиям безопасности информации // Известия Института инженерной физики. 2009. Т. 2. № 12. С. 2–6.
6. Марков А., Никулин М., Цирлов В. Сертификация средств защиты персональных данных: революция или эволюция // Защита информации. Инсайд. 2008. № 5 (23). С. 20–25.
7. Барабанов А.В., Марков А.С., Цирлов В.Л., Корсунский А.С. Инспекционный контроль за стабильностью характеристик сертифицированных средств защиты информации // Автоматизация процессов управления. 2012. № 1. С. 10–14.
8. Аветисян А.И., Белеванцев А.А., Чукляев И.И. Технологии статического и динамического анализа уязвимостей программного обеспечения // Вопросы кибербезопасности. 2014. № 3 (4). С. 20–28.
9. Марков А.С., Миронов С.В., Цирлов В.Л. Выявление уязвимостей программного обеспечения в процессе сертификации // Известия Южного федерального университета. Технические науки. 2006. № 7 (62). С. 82–87.
10. Марков А.С., Цирлов В.Л. Опыт выявления уязвимостей в зарубежных программных продуктах // Вопросы кибербезопасности. 2013. № 1 (1). С. 42–48.
11. Осовецкий Л.Г. Технология выявления недекларированных возможностей при сертификации промышленного программного обеспечения по требованиям безо-

References

1. Pavel M. Komu nuzhna sertifikatsiia?, Information Security, 2014, No. 6, pp. 40-41.
2. Kostogryzov A.I., Lipaev V.V. Sertifikatsiia funktsionirovaniia avtomatizirovannykh informatsionnykh sistem, M.: Izd. “Vooruzhenie. Politika. Konversiia”, 1996, 280 pp.
3. Markov A., Tsirlov V. Sertifikatsiia programm: mify i real’nost’, Otkrytye sistemy, SUBD, 2011, No. 6, pp. 26-29.
4. Metody otsenki nesootvetstviia sredstv zashchity informatsii, A.S. Markov, V.L. Tsirlov, A.V. Barabanov, pod red. A. S. Markova, M.: Radio i sviaz’, 2012, 192 s.
5. Markov A.S., Tsirlov V.L., Maslov V.G., Oleksenko I.A. Testirovanie i ispytaniia programmnogo obespecheniia po trebovaniiam bezopasnosti informatsii, Izvestiia Instituta inzhenernoi fiziki, 2009, t. 2, No. 12, pp. 2-6.
6. Markov A., Nikulin M., Tsirlov V. Sertifikatsiia sredstv zashchity personal’nykh dannykh: revoliutsiia ili evoliutsiia, Zashchita informatsii, Insaid, 2008, No. 5 (23), pp. 20-25.
7. Barabanov A.V., Markov A.S., Tsirlov V.L., Korsunskii A.S. Inspektsionnyi kontrol’ za stabil’nost’iu kharakteristik sertifitsirovannykh sredstv zashchity informatsii, Avtomatizatsiia protsessov upravleniia, 2012, No. 1, pp. 10-14.
8. Avetisian A.I., Belevantsev A.A., Chukliaev I.I. Tekhnologii staticheskogo i dinamicheskogo analiza uiazvimostei programmnogo obespecheniia, Voprosy kiberbezopasnosti, 2014, No. 3 (4), pp. 20-28.
9. Markov A.S., Mironov S.V., Tsirlov V.L. Vyiavlenie uiazvimostei programmnogo obespecheniia v protsesse sertifikatsii, Izvestiia Iuzhnogo federal’nogo universiteta, Tekhnicheskie nauki, 2006, No. 7 (62), pp. 82-87.
10. Markov A.S., Tsirlov V.L. Opyt vyiavleniia uiazvimostei v zarubezhnykh programmnykh produktakh, Voprosy kiberbezopasnosti, 2013, No. 1 (1), pp. 42-48.
11. Osovetskii L.G. Tekhnologiia vyiavleniia nedeklarirovannykh vozmozhnostei pri sertifikatsii promyshlennogo programmnogo obespecheniia po trebovaniiam bezopasnosti informatsii, Voprosy kiberbezopasnosti, 2015, No. 1 (9), pp. 60-64.

пасности информации // Вопросы кибербезопасности. 2015. № 1 (9). С. 60–64.
12. Барабанов В., Марков А.С., Цирлов В.Л. Методический аппарат оценки соответствия автоматизированных систем требованиям безопасности информации // Спецтехника и связь. 2011. № 3. С. 48–52.
13. Марков А.С. Оценка соответствия средств защиты информации требованиям по безопасности информации: смена парадигмы // В сборнике: Информационные технологии и системы. Труды Четвертой Международной научной конференции. / Отв. ред. Ю.С. Попков, А.В. Мельников. Челябинск, 2015. С. 134–136.
14. Барабанов А.В., Марков А.С., Цирлов В.Л. Оценка соответствия средств защиты информации "Общим критериям" // Информационные технологии. 2015. Т. 21. № 4. С. 264–270.
15. Барабанов А., Марков А., Цирлов В. Сертификация систем обнаружения вторжений // Открытые системы. СУБД. 2012. № 3. С. 31–33.
16. Барабанов А.В., Марков А.С., Цирлов В.Л. Сертификация средств антивирусной защиты по новым требованиям безопасности информации // Инженерный журнал: наука и инновации. 2012. № 3 (3). С. 37.
17. Барабанов А.В. Стандартизация процесса разработки безопасных программных средств // Вопросы кибербезопасности. 2013. № 1 (1). С. 37–41.
18. Шахалов И.Ю. Лицензирование деятельности по технической защите конфиденциальной информации // Вопросы кибербезопасности. 2013. № 1 (1). С. 49–54.
19. Шахалов И.Ю. Лицензия как продукт осознанной необходимости лицензирование деятельности операторов персональных данных // Защита информации. Инсайд. 2010. № 2 (32). С. 53–55.
20. Агафонова М.Е., Шахалов И.Ю. К вопросу о проведении внутреннего аудита системы менеджмента информационной безопасности // Вопросы кибербезопасности. 2013. № 3. С. 2–7.
21. Чобанян В.А., Шахалов И.Ю. Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры // Вопросы кибербезопасности. 2013. № 1 (1). С. 17–27.

12. Barabanov V., Markov A.S., Tsirlov V.L. Metodicheskii apparat otsenki sootvetstviia avtomatizirovannykh sistem trebovaniiam bezopasnosti informatsii, Spetstekhnika i sviaz', 2011, No. 3, pp. 48-52.
13. Markov A.S. Otsenka sootvetstviia sredstv zashchity informatsii trebovaniiam po bezopasnosti informatsii: smena paradigmy, v sbornike: Informatsionnye tekhnologii i sistemy, Trudy Chetvertoi Mezhdunarodnoi nauchnoi konferentsii, otv. red. Iu.S. Popkov, A.V. Mel'nikov, Cheliabinsk, 2015, pp. 134-136.
14. Barabanov A.V., Markov A.S., Tsirlov V.L. Otsenka sootvetstviia sredstv zashchity informatsii "Obshchim kriteriiam", Informatsionnye tekhnologii, 2015, t. 21, No. 4, pp. 264-270.
15. Barabanov A., Markov A., Tsirlov V. Sertifikatsiia sistem obnaruzheniia vtorzhenii, Otkrytye sistemy, SUBD, 2012, No. 3, pp. 31-33.
16. Barabanov A.V., Markov A.S., Tsirlov V.L. Sertifikatsiia sredstv antivirusnoi zashchity po novym trebovaniiam bezopasnosti informatsii, Inzhenernyi zhurnal: nauka i innovatsii, 2012, No. 3 (3), pp. 37.
17. Barabanov A.V. Standartizatsiia protsessa razrabotki bezopasnykh programmnykh sredstv, Voprosy kiberbezopasnosti, 2013, No. 1 (1), pp. 37-41.
18. Shakhalov I.Iu. Litsenzirovanie deiatel'nosti po tekhnicheskoi zashchite konfidentsial'noi informatsii, Voprosy kiberbezopasnosti, 2013, No. 1 (1), pp. 49-54.
19. Shakhalov I.Iu. Litsenziia kak produkt osoznannoi neobkhodimosti litsenzirovanie deiatel'nosti operatorov personal'nykh dannykh, Zashchita informatsii, Insaid, 2010, No. 2 (32), pp. 53-55.
20. Agafonova M.E., Shakhalov I.Iu. K voprosu o provedenii vnutrennego audita sistemy menedzhmenta informatsionnoi bezopasnosti, Voprosy kiberbezopasnosti, 2013, No. 3, pp. 2-7.
21. Chobanian V.A., Shakhalov I.Iu. Analiz i sintez trebovanii k sistemam bezopasnosti ob"ektov kriticheskoi informatsionnoi infrastruktury, Voprosy kiberbezopasnosti, 2013, No. 1 (1), pp. 17-27.