

ПОСТАНОВЛЕНИЕ
КАБИНЕТА МИНИСТРОВ РЕСПУБЛИКИ УЗБЕКИСТАН

472 **О мерах по реализации постановления Президента Республики Узбекистан от 8 июля 2011 года № ПП-1572 «О дополнительных мерах по защите национальных информационных ресурсов»**

В целях обеспечения реализации постановления Президента Республики Узбекистан от 8 июля 2011 года № ПП-1572 «О дополнительных мерах по защите национальных информационных ресурсов» Кабинет Министров **постановляет:**

1. Утвердить:

Положение о порядке выдачи разрешения на проведение работ по аттестации объектов информатизации согласно приложению № 1.

Перечень сведений, отнесенных к конфиденциальной информации согласно приложению № 2.

2. Внести изменения и дополнения в некоторые решения Правительства Республики Узбекистан согласно приложению № 3.

3. Контроль за исполнением настоящего постановления возложить на заместителя Премьер-министра Республики Узбекистан А.Н. Арипова.

**Премьер-министр
Республики Узбекистан**

Ш. МИРЗИЁЕВ

г. Ташкент,
7 ноября 2011 г.,
№ 296

ПРИЛОЖЕНИЕ № 1
к постановлению Кабинета Министров
от 7 ноября 2011 года № 296

ПОЛОЖЕНИЕ
о порядке выдачи разрешения на проведение работ
по аттестации объектов информатизации

І. Общие положения

1. Настоящее Положение в соответствии с постановлением Президента Республики Узбекистан от 8 июля 2011 г. № ПП-1572 «О дополнительных мерах по защите национальных информационных ресурсов» определяет порядок выдачи организациям разрешения на право проведения работ по ат-

тестации объектов информатизации на соответствие требованиям информационной безопасности (далее — разрешение).

2. В настоящем Положении используются следующие основные понятия:

объект информатизации — информационные системы различного уровня и назначения, сети телекоммуникаций, технические средства обработки информации, помещения, где установлены и эксплуатируются эти средства, а также отдельные помещения, предназначенные для ведения переговоров, в т. ч. конфиденциальных;

аттестация объектов информатизации — комплекс организационно-технических мероприятий, направленных на определение соответствия фактического состояния защищенности объектов информатизации требованиям государственных стандартов и нормативно-правовых актов в области информационной безопасности;

уполномоченный орган — Служба национальной безопасности Республики Узбекистан;

орган по аттестации — организации, имеющие разрешение уполномоченного органа на проведение определенных видов работ по аттестации объектов информатизации.

3. Разрешение выдается уполномоченным органом.

4. Выдача разрешения осуществляется на основе результатов изучения и оценки возможностей организации, подавшей заявление на получение разрешения (далее — организация-заявитель), на соответствие предъявляемым требованиям.

5. Разрешение является документом, удостоверяющим право организации на проведение определенных видов работ по аттестации объектов информатизации (далее — работы по аттестации). В разрешении указывается срок его действия, но не более чем 5 лет.

6. Разрешение выдается если организация-заявитель имеет:

в собственности, на праве хозяйственного ведения, оперативного управления или на ином законном основании имущество и оборудование, необходимые для проведения работ по аттестации;

в штате специалистов, прошедших специальную подготовку в области информационной безопасности и защиты информации, отдельная категория из которых имеет оформленный в установленном законодательством порядке допуск к государственным секретам;

необходимые нормативно-правовые акты и иные документы для проведения аттестации объектов информатизации.

II. Порядок выдачи и получения разрешения

7. Для получения разрешения организация-заявитель направляет заявление о выдаче разрешения в уполномоченный орган по форме согласно приложению № 1 к настоящему Положению.

8. К заявлению прилагается справка, содержащая:

перечень и характеристики объектов организации-заявителя (основных зданий и сооружений, испытательных лабораторий, безэховых камер, технологических участков, хранилищ и т. п.), с использованием которых планируется проведение работ по аттестации;

сведения о составе и квалификации работников организации;

перечень и характеристики имеющегося оборудования, приборов, аппаратуры с указанием года выпуска и наличия сертификатов соответствия;

перечень и характеристики имеющейся измерительной техники с указанием года выпуска и прохождения поверки в установленном законодательством порядке;

сведения о наличии лицензионного программного обеспечения;

сведения о наличии службы безопасности в организации-заявителе;

перечень документов, устанавливающих общие и специальные требования по обеспечению информационной безопасности в организации-заявителе;

описание структуры организации-заявителя;

перечень имеющихся в наличии государственных стандартов, нормативно-правовых актов и иных документов по информационной безопасности.

К справке прилагаются копии:

учредительного документа организации-заявителя;

документа о государственной регистрации организации-заявителя;

лицензии, дающей право на проведение отдельных видов работ (если имеется);

документов, подтверждающих наличие имущества и оборудования, необходимого для проведения работ по аттестации;

должностных инструкций работников, привлекаемых или планируемых к привлечению для выполнения работ по аттестации.

9. Документы, представляемые организацией-заявителем, должны быть оформлены в соответствии с требованиями, установленными законодательством.

10. Уполномоченный орган в течение 30 календарных дней рассматривает заявление, справку и прилагаемые к ней материалы и направляет организации-заявителю письменное извещение о принятии его к дальнейшему рассмотрению с указанием суммы сбора. В случае отклонения заявления направляется извещение с указанием причин его отклонения.

11. Заявление отклоняется от рассмотрения:

при несоответствии представленных документов требованиям пунктов 6, 8 и 9 настоящего Положения;

если заявленная деятельность не соответствует уставу (положению) организации.

12. Рассмотрение справки и прилагаемых к ней материалов проводится в течение 2 месяцев с даты направления организации — заявителю извещения о приеме заявления к рассмотрению.

13. В процессе рассмотрения справки и прилагаемых к ней материалов уполномоченный орган проводит проверку наличия необходимых условий, требуемых для проведения работ по аттестации.

14. Основанием для отказа в выдаче разрешения является:

недостаточность или отсутствие у организации условий, указанных в пунктах 6 и 8 настоящего Положения;

наличие в заявлении недостоверной или искаженной информации.

15. Порядок оплаты работ, связанных с выдачей разрешения, определяется уполномоченным органом. Сумма сбора за рассмотрение справки и прилагаемых к ней материалов определяется в пределах затрат уполномоченного органа, связанных с выдачей данного разрешения и используется на покрытие этих затрат.

Сумма сбора зачисляется на счет уполномоченного органа. В случае отзыва заявления или принятия уполномоченным органом решения об отказе в выдаче разрешения сумма уплаченного сбора возврату не подлежит.

16. Вместе с разрешением органу по аттестации выдается пакет рабочих документов, стоимость которых входит в сумму сбора, взимаемого за рассмотрение заявления о выдаче разрешения.

17. Разрешение оформляется на специальном бланке, имеющем учетную серию, номер и соответствующую степень защиты, по форме согласно приложению № 2 к настоящему Положению.

Уполномоченный орган ведет учет органов по аттестации.

III. Прекращение и приостановление действия разрешения

18. Уполномоченный орган вправе прекратить действие разрешения раньше установленного срока:

по заявлению органа по аттестации;

при ликвидации органа по аттестации.

19. В случае подачи органом по аттестации заявления о досрочном прекращении своей деятельности по аттестации уполномоченный орган отзывает разрешение. Заявление подается не позднее 30 календарных дней до предполагаемой даты прекращения деятельности.

20. В случае нарушения органом по аттестации предъявляемых к нему требований уполномоченный орган вправе применить меры по прекращению и/или приостановлению действия выданного разрешения в соответствии с законодательством.

21. При принятии решения о приостановлении или прекращении действия разрешения в соответствии с законодательством уполномоченный орган направляет органу по аттестации официальное уведомление.

IV. Переоформление разрешения, продление срока его действия, выдача дубликата

22. В случаях изменения наименования, местонахождения (почтового адреса), преобразования орган по аттестации обязан в недельный срок подать в уполномоченный орган заявление о переоформлении разрешения с приложением документов, подтверждающих указанные изменения.

23. Продление срока действия разрешения осуществляется по заявлению органа по аттестации.

Заявление о продлении срока действия разрешения должно быть подано в уполномоченный орган не позднее трех месяцев до истечения срока действия разрешения.

Порядок оплаты работ, связанных с продлением срока действия разрешения, определяется уполномоченным органом. Сумма сбора определяется в пределах затрат уполномоченного органа, связанных с продлением данного разрешения, и используется на покрытие этих затрат.

24. Взамен утраченного или пришедшего в негодность разрешения, срок действия которого не истек, по заявлению органа по аттестации выдается дубликат. За выдачу дубликата сбор не взимается.

ПРИЛОЖЕНИЕ № 1
к Положению о порядке выдачи разрешения на проведение работ по аттестации объектов информатизации

Образец формы заявления
(на фирменном бланке заявителя)

Служба национальной
безопасности Республики Узбекистан

ЗАЯВЛЕНИЕ
о выдаче разрешения на проведение работ по аттестации
объектов информатизации на соответствие требованиям
информационной безопасности

_____ просит выдать
(полное и сокращенное наименование организации)
разрешение на право проведения работ по аттестации объектов информатизации на соответствие требованиям информационной безопасности на срок до «___» _____ 20__ г.

Оплату гарантируем.

Почтовый адрес:
Банковские реквизиты:
Телефон:
Факс:
E-mail:

Приложения: _____
(по перечню документов, предусмотренному в пункте 8 Положения о порядке выдачи разрешения на проведение работ по аттестации объектов информатизации).

М.П. _____
(подпись руководителя организации и дата)

(подпись главного бухгалтера организации и дата)

ПРИЛОЖЕНИЕ № 2
к Положению о порядке выдачи разреше-
ния на проведение работ по аттестации
объектов информатизации

**Образец формы разрешения на проведение работ
по аттестации объектов информатизации на соответствие
требованиям информационной безопасности**
(выполняется на специальном бланке Уполномоченного органа)

РАЗРЕШЕНИЕ № _____

Выдано «___» _____ 20__ г. _____
(наименование организации)

Настоящим разрешением _____
(наименование организации)

предоставляется право на проведение работ по аттестации объектов инфор-
матизации на соответствие требованиям информационной безопасности.

Исключение составляют объекты информатизации: _____

_____.

Разрешение выдано на основании заявления от «___» _____ 20__ года
№ _____.

Почтовый адрес организации: _____
_____.

Срок действия разрешения: с «___» _____ 20__ г. по
«___» _____ 20__ г.

Разрешенная деятельность должна осуществляться в соответствии с
законодательством, государственными стандартами и нормативно-правовы-
ми актами, распространяющимися на осуществляемую деятельность, а так-
же условиями действия настоящего разрешения, являющимися его неотъем-
лемой частью.

В случае нарушения органом по аттестации предъявляемых к нему тре-
бований уполномоченный орган вправе применить меры по прекращению
и/или приостановлению действия выданного разрешения в соответствии с
законодательством.

В случае появления новых факторов, влияющих на надлежащее выпол-

нение заявленной деятельности, уполномоченный орган может откорректировать условия действия разрешения.

При ликвидации организации действие разрешения прекращается.

Государственный надзор за выполнением условий действия разрешения осуществляет уполномоченный орган.

Ответственное лицо
от уполномоченного органа

_____ (подпись и дата)

М.П.

ПРИЛОЖЕНИЕ № 2
к постановлению Кабинета Министров
от 7 ноября 2011 года № 296

**ПЕРЕЧЕНЬ
сведений, отнесенных к конфиденциальной информации**

1. Информация о персональных данных физических лиц.
2. Информация о частной жизни, равно как информация, нарушающая тайну частной жизни физического лица, за исключением случаев, установленных законодательством.
3. Информация об источнике информации или авторе, подписавшемся псевдонимом, за исключением случаев, установленных законодательством.
4. Сведения о тайне переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям телекоммуникаций, доступ к которым ограничен в соответствии с законодательством.
5. Сведения, составляющие тайну следствия и судопроизводства, доступ к которым ограничен в соответствии с законодательством.
6. Служебные сведения, доступ к которым ограничен обладателем информации в соответствии с законодательством.
7. Информация, составляющая коммерческую тайну, доступ к которой ограничен в соответствии с законодательством.
8. Банковская тайна, тайны страхования личности и завещания, доступ к которым ограничен в соответствии с законодательством.
9. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с законодательством (врачебная тайна, тайна нотариальных действий, адвокатская тайна и т. п.).
10. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

ПРИЛОЖЕНИЕ № 3
к постановлению Кабинета Министров
от 7 ноября 2011 года № 296

Изменения и дополнения, вносимые в некоторые решения Правительства Республики Узбекистан

1. Пункт 4 раздела II Положения о Службе национальной безопасности Республики Узбекистан, утвержденного постановлением Кабинета Министров от 2 ноября 1991 г. № 278 (СП Республики Узбекистан, 1991 г., № 11, ст. 38), изложить в следующей редакции:

«4. Участвуют в разработке и осуществлении мер по защите государственных секретов и конфиденциальной информации на народнохозяйственных и других объектах; формируют и реализуют государственную политику, осуществляют государственный контроль в сфере криптографической и технической защиты информации; обеспечивают стандартизацию, сертификацию и лицензирование деятельности в области криптографической и технической защиты информации, совершенствуют нормативно-правовую базу в данной сфере; определяют приоритетные направления научно-исследовательских и опытно-конструкторских работ в области развития систем криптографической и технической защиты информации, разрабатывают и осуществляют мероприятия по их реализации; формируют и совершенствуют систему подготовки квалифицированных кадров в области криптографической и технической защиты информации; осуществляют мероприятия в области организации Системы аттестации объектов информатизации».

2. В Положении о порядке подготовки и распространения информационных ресурсов Республики Узбекистан на сети передачи данных, включая Интернет, утвержденном постановлением Кабинета Министров от 26 марта 1999 г. № 137 (СП Республики Узбекистан, 1999 г., № 3, ст. 17):

а) абзац третий пункта 5 изложить в следующей редакции:

«Конфиденциальная информация — документированная информация, не содержащая информацию, отнесенную к государственным секретам, доступ к которой ограничивается в соответствии с законодательством»;

б) пункт 12.2 изложить в следующей редакции:

«12.2. Включение в состав средств информационного обмена государственных информационных систем, сетей, для которых установлены особые правила доступа к информационным ресурсам, осуществляется с разрешения Кабинета Министров Республики Узбекистан после проведения аттестации в соответствии с требованиями информационной безопасности»;

в) пункт 19 дополнить абзацем следующего содержания:

«Обязательной аттестации в соответствии с требованиями информационной безопасности подлежат информационные системы, предназначенные для формирования государственных информационных ресурсов, содержащих информацию ограниченного доступа».

3. Положение о порядке создания информационных систем государствен-

ных органов, утвержденное постановлением Кабинета Министров от 22 ноября 2005 г. № 256 (СП Республики Узбекистан, 2005 г., №11, ст. 62), дополнить пунктом 28¹ следующего содержания:

«28¹. Информационные системы государственных органов, предназначенные для обработки информации, отнесенной к государственным секретам или конфиденциальной информации, подлежат обязательной аттестации в соответствии с требованиями информационной безопасности в установленном законодательством порядке».