

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования **«МИРЭА – Российский технологический университет»  
РТУ МИРЭА**

**Институт кибербезопасности и цифровых технологий**

*(наименование института, филиала)*

**Кафедра КБ-2«Прикладные информационные технологии»**

*(наименование кафедры)*

**ОТЧЕТ**

по дисциплине: «Основы информационной безопасности»

Работа с правовыми актами, документами и стандартами ИБ

*(задание)*

Задание получил:

|  |  |
| --- | --- |
| 1 курс, группа БИСО-02-2023 | 23Б0980 |
|  | *Шифр* |

|  |
| --- |
| \_\_\_\_\_\_\_\_ Макаревич Сергей В.\_\_\_\_\_\_\_\_\_\_\_ |
| *ФИО* |

Проверил:

|  |  |
| --- | --- |
| « » 2023 г. |  |
| *Дата* | *Подпись* |

|  |  |
| --- | --- |
|  |  |
| *Отметка / результат* | *ФИО* |

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ………….………………………………………………………. 2  
ВВЕДЕНИЕ………….…………………………………………………………… 3

[1 РАБОТА №1 4](#_Toc147939070)

[1.1 Теоретические вопросы. 4](#_Toc147939071)

[1.2 перечень основных норм, активных документов, регламентирующих деятельность области защиты информации: 4](#_Toc147939072)

[1.3 Задание 1. 13](#_Toc147939081)

[1.4 Задание 2. 14](#_Toc147939082)  
 [1.5 Задание 3. 15](#_Toc147939083)  
 [1.6 Задание 4. 17](#_Toc147939084)

[СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ 20](#_Toc147939085)

**Введение**

Была поставлена задача научиться работать в справочно-правовой системе с нормативными и правовыми документами по защите информации, а также провести обзор стандартов защиты информации и поработать с их содержанием.

Для этого следует выполнить две работы по дисциплине «Основы информационной безопасности» и познакомиться с правовыми документами, методическими документами по защите информации программно-аппаратными средствами, а также разобраться в стандартах по защите информации.

Перейдем к первой работе.

# 1 РАБОТА №1

## 1.1 Теоретические вопросы.

1.  Предмет и задачи программно-аппаратной защиты информации.

2.  Основные понятия программно-аппаратной защиты информации.

3.  Классификация методов и средств программно-аппаратной защиты информации.

4.  Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

## 1.2 перечень основных норм, активных документов, регламентирующих деятельность области защиты информации:

## 1) Конституция РФ

## Статья 22.

## Каждый имеет право на свободу и личную неприкосновенность. Статья 23

## Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

## Статья 24.

## Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

## Статья 29

## Конституции России гарантирует жителям страны возможность искать, получать, передавать, производить, распространять информацию, если таковая не является информацией с ограниченным доступом, или не наносит вред интересам иных лиц.

**2) Гражданский кодекс Российской Федерации**

**Статья 152. Защита чести, достоинства и деловой репутации**

1. Гражданин вправе требовать по суду [опровержения](https://www.consultant.ru/document/cons_doc_LAW_52017/#dst100020) порочащих его честь, достоинство или деловую репутацию [сведений](https://www.consultant.ru/document/cons_doc_LAW_52017/#dst100032), если распространивший такие сведения не докажет, что они соответствуют действительности.

2. Сведения, порочащие честь, достоинство или деловую репутацию гражданина и распространенные в средствах массовой информации, должны быть опровергнуты в тех же средствах массовой информации.

3. В случаях, когда сведения, порочащие честь, достоинство или деловую репутацию гражданина, стали широко известны и в связи с этим опровержение невозможно довести до всеобщего сведения, гражданин вправе требовать удаления соответствующей информации, а также пресечения или запрещения дальнейшего [распространения](https://www.consultant.ru/document/cons_doc_LAW_52017/#dst100029) указанных сведений путем изъятия и уничтожения без какой бы то ни было компенсации … экземпляров материальных носителей, содержащих указанные сведения

4. Если сведения, порочащие честь, достоинство или деловую репутацию гражданина, оказались после их распространения доступными в сети "Интернет", гражданин вправе требовать удаления соответствующей информации,

**Статья 152.1. Охрана изображения гражданина**

1. Обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) допускаются только с согласия этого гражданина. После смерти гражданина его изображение может использоваться только с согласия детей и пережившего супруга, а при их отсутствии - с согласия родителей. Такое согласие не требуется в случаях, когда:

1) использование изображения осуществляется в государственных, общественных или иных публичных интересах;

2) изображение гражданина получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и подобных мероприятиях), за исключением случаев, когда такое изображение является основным объектом использования;

**Статья 152.2. Охрана частной жизни гражданина**

1. Если иное прямо не предусмотрено законом, не допускаются без согласия гражданина сбор, хранение, распространение и использование любой информации о его частной жизни, в частности сведений о его происхождении, о месте его пребывания или жительства, о личной и семейной жизни.

Не являются нарушением правил, установленных абзацем первым настоящего пункта, сбор, хранение, распространение и использование информации о частной жизни гражданина в государственных, общественных или иных публичных интересах, а также в случаях, если информация о частной жизни гражданина ранее стала общедоступной либо была раскрыта самим гражданином или по его воле.

2. Стороны обязательства не вправе разглашать ставшую известной им при возникновении и (или) исполнении обязательства информацию о частной жизни гражданина, являющегося стороной или третьим лицом в данном обязательстве, если соглашением не предусмотрена возможность такого разглашения информации о сторонах.

3. Неправомерным распространением полученной с нарушением закона информации о частной жизни гражданина считается, в частности, ее использование при создании произведений науки, литературы и искусства, если такое использование нарушает интересы гражданина.

4. В случаях, когда информация о частной жизни гражданина, полученная с нарушением закона, содержится в документах, видеозаписях или на иных материальных носителях, гражданин вправе обратиться в суд с требованием об удалении соответствующей информации, а также о пресечении или запрещении дальнейшего ее распространения путем изъятия и уничтожения без какой бы то ни было компенсации изготовленных в целях введения в гражданский оборот экземпляров материальных носителей, содержащих соответствующую информацию, если без уничтожения таких экземпляров материальных носителей удаление соответствующей информации невозможно.

5. Право требовать защиты частной жизни гражданина способами, предусмотренными пунктом 2 статьи 150 настоящего Кодекса и настоящей статьей, в случае его смерти имеют дети, родители и переживший супруг такого гражданина.

**3) Уголовный Кодекс РФ**

**Глава 28. Преступления в сфере компьютерной информации**

**Статья 272.** [**Неправомерный доступ к компьютерной информации**](https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/)

[Неправомерный доступ](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100022) к охраняемой законом компьютерной информации, [копирование](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100028) компьютерной информации наказывается.

**Статья 273.** [**Создание, использование и распространение вредоносных компьютерных программ**](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/)

1. [Создание](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100040), [распространение](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100041) или [использование](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100042) компьютерных [программ](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100036) либо иной [компьютерной информации](https://www.consultant.ru/document/cons_doc_LAW_422137/5c337673c261a026c476d578035ce68a0ae86da0/#dst978), заведомо предназначенных для несанкционированного [уничтожения](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100025), [блокирования](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100026), [модификации](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100027), [копирования](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100028) компьютерной информации или нейтрализации средств защиты компьютерной информации, - наказываются

**Статья 274.2. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования.**

Нарушение порядка установки, эксплуатации и модернизации в сети связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования либо несоблюдение технических условий их установки или требований к сетям связи при использовании указанных технических средств … наказывается.

1. **Доктрина информационной безопасности РФ**

1. Настоящая Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

В настоящей Доктрине под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Определяет следующие национальные интересы в информационной сфере:

1. Обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации;
2. Обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры;
3. Развитие в Российской Федерации отрасли информационных технологий и электронной промышленности;
4. Содействие формированию системы международной информационной безопасности. (Глава I, п. 8)

**Главой III определяет основные информационные угрозы:**

1. Наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях;
2. Расширение масштабов использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств.
3. Наращивание информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.
4. Увеличение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий.

Главой IV определяются цели и основные направления обеспечения информационной безопасности: защита жизненно важных интересов личности, прогнозирование информационных угроз, сдерживание и предотвращение военных конфликтов, защита суверенитета и поддержание политической и социальной стабильности, территориальной целостности Российской Федерации.

1. **Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1**

Ст. 5 определяет перечень сведений, составляющих государственную тайну:

1. Сведения в военной области: о содержании стратегических планов, о планах строительства ВС РФ, о разработке, производстве и утилизации ядерных боеприпасов, о дислокации, назначении и степени готовности особо важных объектов и др.
2. Сведения в области экономики, науки и техники: о силах и средствах гражданской обороны, об объемах государственного оборонного заказа, о достижениях науки и техники, о запасах металлов платиновой группы и др.
3. Сведения в области внешней политики и экономики: о внешнеполитической и внешнеэкономической деятельности Российской Федерации, о финансовой политике в отношении иностранных государств, о расходах федерального бюджета и др.

Ст. 20 определяет органы защиты государственной тайны: межведомственная комиссия по защите государственной тайны, органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны и др.

Ст. 26 устанавливается ответственность за нарушение законодательства РФ о государственной тайне: [уголовную](https://www.consultant.ru/document/cons_doc_LAW_2481/657ef9e1c9186c9333add5e1e7ed15b09d652323/), [административную](https://www.consultant.ru/document/cons_doc_LAW_2481/657ef9e1c9186c9333add5e1e7ed15b09d652323/), гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.

**6) Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ**

Ст.3 определяются принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации. Оно основывается на свободе поиска, производства и распространения информации, установлении ограничений доступа к информации только федеральными законами, открытости информации о деятельности государственных органов и др.

Ст.12 описываются области государственного регулирования в сфере применения информационных технологий: регулирование отношений, связанных с поиском, производством и получением информации с применением информационных технологий, развитие информационных систем различного назначения для обеспечения граждан.

Ст.16 описывает способы защиты информации. Среди них принятие правовых, организационных и технических мер, направленных на: обеспечение защиты информации от неправомерного доступа, копирования, распространения и др. неправомерных действий в отношении информации, соблюдение конфиденциальности информации ограниченного доступа, реализация права на доступ к информации.

**7) Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ**

Ст.3 определяются основные понятия, используемые в федеральном законе: персональные данные, оператор, обработка персональных данных, обезличивание персональных данных и др.

Ст.6 устанавливаются условия обработки персональных данных: осуществляется с согласия субъекта персональных данных на обработку его персональных данных, необходима для защиты жизни, здоровья и иных жизненно важных интересов субъекта.

Ст.24 предусматривается ответственность за нарушение требований настоящего Федерального закона. Моральный вред, причинённый субъекту, подлежит возмещению в соответствии с законодательством Российской Федерации.

**8) Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ**

Ст.2 определяются основные понятия, используемые в федеральном законе: электронная подпись(информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию), сертификат ключа проверки электронной подписи (электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи), ключ электронной подписи, удостоверяющий центр и др.

Ст.3 устанавливается правовое регулирование отношений в области использования электронных подписей.

**9) Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ**

Ст.3 определяются основные понятия, используемые в федеральном законе: коммерческая тайна(режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду), контрагент(сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию) и др.

Ст.10 устанавливает меры по охране конфиденциальности информации, принимаемые ее обладателем: определение перечня информации, составляющей коммерческую тайну, учет лиц, получивших доступ к информации, ограничение доступа к информации, составляющей коммерческую тайну.

Ст.14 предусматривается ответственность за нарушение требований настоящего Федерального закона: [дисциплинарную](https://www.consultant.ru/document/cons_doc_LAW_48699/7bf74106889c69a20807dccd2432bf93fd7465f7/), [гражданско-правовую,](https://www.consultant.ru/document/cons_doc_LAW_48699/7bf74106889c69a20807dccd2432bf93fd7465f7/) [административную](https://www.consultant.ru/document/cons_doc_LAW_411165/835dca84f369ce440288da07465dbbf24791784a/#dst101154) или [уголовную](https://www.consultant.ru/document/cons_doc_LAW_422137/696074503229a6bf1978651f48895bf3a8831bd8/#dst101135) ответственность в соответствии с законодательством Российской Федерации.

**10) Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне»**

Определяет [перечень сведений, отнесенных к государственной тайне](https://www.consultant.ru/document/cons_doc_LAW_8522/447b0198c5818883f33364e226f21c3c7329d4f9/): с[ведения в военной области](https://www.consultant.ru/document/cons_doc_LAW_8522/3f757850dd7fbfc5d0520fc664f86ccc6b2e0688/), с[ведения в области экономики, науки и техники](https://www.consultant.ru/document/cons_doc_LAW_8522/ab681baaa0bde79a653ecece91169998147b4ce9/), с[ведения в области внешней политики и экономики](https://www.consultant.ru/document/cons_doc_LAW_8522/899d8c7c4d49cf7963702eb8f851f9886fd73ddf/), с[ведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, в области противодействия терроризму и обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты](https://www.consultant.ru/document/cons_doc_LAW_8522/2f437520b6375e0417a9ea40428bb8b5399b9262/).

**11) Указ Президента РФ от 6 марта 1997 г. №188 «Об утверждении перечня сведений конфиденциального характера»**

Определяет перечень сведений, относящихся к сведениям конфиденциального характера: Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, служебные сведения, сведения о коммерческой деятельности, личные дела осужденных и т.д.

**12) Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»**

Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных (далее - информационные системы) и уровни защищенности таких данных.

Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных.

Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

**13) Постановление Правительства РФ от 03.02.2012 N 79 (ред. от 26.11.2021) "О лицензировании деятельности по технической защите конфиденциальной информации" (вместе с "Положением о лицензировании деятельности по технической защите конфиденциальной информации")**

Определяет порядок лицензирования деятельности по технической защите конфиденциальной информации, осуществляемой юридическими лицами и индивидуальными предпринимателями.

При осуществлении лицензируемого вида деятельности лицензированию подлежат: услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам, услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации, услуги по мониторингу информационной безопасности средств и систем информатизации, работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации, услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации.

**14) Приказ от 11 февраля 2013г. № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"**

В документе устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информации в целях ее добывания, уничтожения, искажения или блокирования доступа к ней при обработке указанной информации в государственных информационных системах.

Определяет требования к организации защиты информации, содержащейся в информационной системе: разработка системы защиты, аттестация информационной системы и ввод ее в действие, обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы, ограничения программной среды, защита машинных носителей информации, обнаружение вторжение, защита среды виртуализации, защита технических средств.

**15) Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»**

Определяет состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий. В него входят:

1. идентификация и аутентификация субъектов доступа и объектов доступа;
2. управление доступом субъектов доступа к объектам доступа, ограничение программной среды;
3. защита машинных носителей информации, на которых хранятся и обрабатываются персональные данные, регистрация событий безопасности, антивирусная защита, обнаружение (предотвращение) вторжений, контроль (анализ) защищенности персональных данных, обеспечение целостности информационной системы и персональных данных, обеспечение доступности персональных данных, защита среды виртуализации и др.

**Руководящие документы ФСТЭК по защите от НСД**

**Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г.**

Устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов.

Необходимыми исходными данными для проведения классификации конкретной АС являются:

1. перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
2. перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
3. матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
4. режим обработки данных в АС.

**Руководящие документы ФСТЭК по защите от НДВ**

**Приказ председателя Гостехкомиссии России от 4 июня 1999 г. N 114**

Устанавливает классификацию программного обеспечения (ПО), защиты информации (СЗИ), в том числе и встроенных в общесистемное и прикладное ПО.

Документ предназначен для специалистов испытательных лабораторий, заказчиков, разработчиков ПО СЗИ при его контроле в части отсутствия не декларированных возможностей.

**Положение по аттестации объектов информатизации по требованиям безопасности информации от 25 ноября 1994 г.**

Устанавливает основные принципы, организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.

**Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)**

Устанавливает порядок организации работ, требования и рекомендации по обеспечению технической защиты конфиденциальной информации на территории Российской Федерации и является основным руководящим документом в этой области для федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, предприятий, учреждений и организаций, должностных лиц и граждан Российской Федерации, взявшим на себя обязательства либо обязанными по статусу исполнять требования правовых документов Российской Федерации по защите информации.

# 1.3 Задание 1.

Нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами:

1. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ
2. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ
3. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
4. ФСТЭК: Приказ от 11 февраля 2013г. № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"  
   Руководящие документы ФСТЭК по защите от НСД
5. Руководящие документы ФСТЭК по защите от НДВ
6. Федеральный закон от 31.07.2023 N 408-ФЗ "О внесении изменения в Федеральный закон "Об информации, информационных технологиях и о защите информации"

# 1.4 Задание 2.

Требования и рекомендации по защите информации программными и программно-аппаратными средствами:

1. Граждане (физические лица) и организации (юридические лица) (далее - организации) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами (ст.3)
2. В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации (ст.10)
3. Случаи и условия обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются федеральными [законами](http://www.consultant.ru/document/cons_doc_LAW_416262/) (ст.10)
4. Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица. (ст.10)
5. Государственное регулирование в сфере применения информационных технологий предусматривает: регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных настоящим Федеральным [законом](http://www.consultant.ru/document/cons_doc_LAW_422054/72898298ae4b1568b5dabf766b3a1bab03748c2a/#dst100028); развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;  
   создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети "Интернет" и иных подобных информационно-телекоммуникационных сетей;  
   обеспечение информационной безопасности детей (ст.12).
6. Права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных (ст.13).
7. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации (ст.16).
8. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:
9. предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
10. своевременное обнаружение фактов несанкционированного доступа к информации;
11. предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
12. недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
13. возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
14. постоянный контроль за обеспечением уровня защищенности информации;
15. нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

# 1.5 Задание 3.

Приказ ФСТЭК России от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Требования и рекомендации по защите информации программными и программно-аппаратными средствами.

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

1. идентификация и аутентификация субъектов доступа и объектов доступа;
2. управление доступом субъектов доступа к объектам доступа;
3. ограничение программной среды;
4. защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
5. регистрация событий безопасности;
6. антивирусная защита;
7. обнаружение (предотвращение) вторжений;
8. контроль (анализ) защищенности персональных данных;
9. обеспечение целостности информационной системы и персональных данных;
10. обеспечение доступности персональных данных;
11. защита среды виртуализации;
12. защита технических средств;
13. защита информационной системы, ее средств, систем связи и передачи данных;
14. выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
15. управление конфигурацией информационной системы и системы защиты персональных данных (п.8)

Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:

1. определение базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных в соответствии с базовыми наборами мер по обеспечению безопасности персональных данных, приведенными в приложении к настоящему документу;
2. адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);
3. уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных с учетом не выбранных ранее мер, приведенных в приложении к настоящему документу, в результате чего определяются меры по обеспечению безопасности персональных данных, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных для конкретной информационной системы;
4. дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации (п.9)
5. могут применяться следующие меры:
6. проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие не декларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;
7. тестирование информационной системы на проникновения;
8. использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования (п.11)

# 1.6 Задание 4.

Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, (утвержденные руководством Центра ФСБ России 21.02.2008 №149/6/6-622.)

Операторы несут ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности обработки с использованием крипто средств персональных данных лицензионным требованиям и условиям, эксплуатационной и технической документации к крипто средствам, а также настоящим Требованиям.

При этом операторы должны обеспечивать комплексность защиты персональных данных, в том числе посредством применения не криптографических средств защиты.

2.3. При разработке и реализации мероприятий по организации и обеспечению безопасности персональных данных при их обработке в информационной системе оператор или уполномоченное оператором лицо осуществляет:

- разработку для каждой информационной системы персональных данных модели угроз безопасности персональных данных при их обработке;

- разработку на основе модели угроз системы безопасности персональных данных, обеспечивающей нейтрализацию всех перечисленных в модели угроз;

- определение необходимости использования крипто средств для обеспечения безопасности персональных данных и, в случае положительного решения, определение на основе модели угроз цели использования крипто средств для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных и (или) иных неправомерных действий при их обработке;

- установку и ввод в эксплуатацию крипто средств в соответствии с эксплуатационной и технической документацией к этим средствам;

- проверку готовности крипто средств к использованию с составлением заключений о возможности их эксплуатации;

- обучение лиц, использующих крипто средства, работе с ними;

- по экземплярный учет используемых крипто средств, эксплуатационной и технической документации к ним, носителей персональных данных;

- учет лиц, допущенных к работе с крипто средствами, предназначенными для обеспечения безопасности персональных данных в информационной системе (пользователи крипто средств);

- контроль за соблюдением условий использования крипто средств, предусмотренных эксплуатационной и технической документацией к ним;

- разбирательство и составление заключений по фактам нарушения условий хранения носителей персональных данных, использования крипто средств, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

- описание организационных и технических мер, которые оператор обязуется осуществлять при обеспечении безопасности персональных данных с использованием крипто средств при их обработке в информационных системах, с указанием в частности:

а) индекса, условного наименования и регистрационных номеров используемых крипто средств;

б) соответствия размещения и монтажа аппаратуры и оборудования, входящего в состав крипто средств, требованиям нормативной документации и правилам пользования крипто средствами;

в) соответствия помещений, в котором размещены крипто средства и хранится ключевая документация к ним, настоящим Требованиям с описанием основных средств защиты;

г) выполнения Требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Описание принятых мер должно быть включено в уведомление, предусмотренное [частью 1](https://normativ.kontur.ru/document?moduleId=1&documentId=184098#l150) статьи 22 Федерального закона "О персональных данных".

# СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Конституция Российской Федерации
2. Уголовный Кодекс Российской Федерации
3. Доктрина информационной безопасности Российской Федерации;
4. Законы Российской Федерации:
   1. Федеральный закон РФ от 21.07.1993 № 5485-1 «О государственной тайне»;
   2. Федеральный закон РФ от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
   3. Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных»;
   4. Федеральный закон РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
   5. Федеральный закон от 29.04.2004 № 98-ФЗ «О коммерческой тайне»;
5. Указы Президента Российской Федерации:
   1. Указ Президента РФ от 30 ноября 1995 г. №1203 «Об утверждении перечня сведений, отнесенных к государственной тайне»;
   2. Указ Президента РФ от 6 марта 1997 г. №188 «Об утверждении перечня сведений конфиденциального характера»;
6. Постановления Правительства Российской Федерации:
   1. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
   2. Постановление Правительства РФ от 03.02.2012 № 79 "О лицензировании деятельности по технической защите конфиденциальной информации";
7. Документы ФСТЭК, ФСБ:
   1. Приказ от 11 февраля 2013г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
   2. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
   3. Руководящие документы ФСТЭК по защите от НСД;
   4. Руководящие документы ФСТЭК по защите от НДВ;
   5. Положение по аттестации объектов информатизации по требованиям безопасности информации от 25 ноября 1994 г.;
   6. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К);
   7. Приказ ФСБ РФ от 9 февраля 2005г. № 66 «Об утверждении, разработке, производстве, реализации и эксплуатации шифровальных и криптографических средств защиты (Положение ПКЗ-2005»).