# МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

# федеральное государственное автономное образовательное учреждение высшего образования

# «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

# АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА №13

ОТЧЕТ ЗАЩИЩЕН С ОЦЕНКОЙ\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ПРЕПОДАВАТЕЛЬ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| доцент |  |  |  | А.А.Свинарчук |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №1

Законодательство РФ в области информационной безопасности

по курсу: Основы информационной безопасности

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| СТУДЕНТ ГР. № | | 1934 |  |  |  | Росляков В.Д. |
|  | номер группы | |  | подпись, дата |  | инициалы, фамилия |

Санкт-Петербург 2022

Цель работы: закрепление теоретических знаний в области правового обеспечения информационной безопасности.

Задача: провести анализ существующих нормативно-правовых актов по информационной безопасности и ответить на контрольные вопросы.

1. **Охарактеризуйте информацию и ее основные показатели**.

В Федеральном законе от 27.07.2006 № 149 статье 2 используются следующие основные понятия:

* информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
* информация – сведения (сообщения, данные) независимо от формы их представления;

Информация может характеризоваться также и «прагматическими» свойствами. Их содержание определяется ролью, значимостью, важностью информации в процессе решения задач, а также количеством и содержанием информации, имеющейся в момент решения соответствующей задачи.

Важно не просто количество сведений в абсолютном выражении, а достаточность (полнота) их для информационного обеспечения решаемых задач и адекватность, то есть соответствие текущему состоянию тех объектов или процессов, к которым относится оцениваемая информация.

Показатели информации: Полнота информации, Адекватность информации, важность информации, релевантность информации, толерантность информации.

1. **Какие существуют подходы к определению понятия «информация».**

Существуют два основных научных подхода к определению того, что такое информация. Первый, информация есть внешнее описание объекта, содержащееся в передаваемом сообщении. Количество информации в этом случае определяется как мера неопределенности, снимаемая полученным сообщением. Согласно второму подходу, информация не связывается с передаваемым сообщением. Она относится к объекту и есть мера разнообразия объекта.

* Федеральный закон от 27.07.2006 № 149.

1. **В чем заключается двуединство документированной информации с правовой точки зрения.**

С правовой точки зрения двуединство информации и материального носителя дает возможность защищать документированную информацию с использованием одновременно двух институтов: института интеллектуальной собственности и института вещной собственности.

Обеспечение безопасности информации, в том числе и в компьютерных системах, требует сохранения следующих ее свойств: целостности; доступности; конфиденциальности.

* Федеральный закон «Об информации, информационных технологиях и о защите информации».

1. **Дайте характеристику следующих видов информации: документированная, конфиденциальная, массовая.**

Документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Массовая информация – предназначенные для неограниченного круга лиц печатные, аудиосообщения, аудиовизуальные и иные сообщения и материалы.

* Ст.2 Федерального закона от 27.07.2006 №149.

1. **К какому виду информации относится записанный на бумаге текст программы для ЭВМ?**

В зависимости от критерия, по которому будут ее оценивать. Если по способу восприятия – визуальная, по назначению – специальная, по форме представления – текстовая.

1. **Назовите основные виды конфиденциальной информации.**

Конфиденциальная информация, как и государственная тайна, относится к информации ограниченного доступа. К видам информации конфиденциального характера относятся: персональные данные, коммерческая тайна, служебная тайна, профессиональная тайна, тайна следствия и судопроизводства.

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

1. **Какие сведения, в соответствии с законодательством, не могут быть отнесены к информации с ограниченным доступом?**

К конфиденциальной информации не должна относиться информация, которая в силу закона запрещена, например, информация, запрещенная законом о противодействии экстремистской деятельности. Кроме того, такая информация не должна присутствовать в документах организации и на ее интернет-сайте. К такой информации может быть, в частности, отнесена информация о террористической деятельности, материалы экстремистской направленности.

* Ст.9 Федерального закона от 27.07.2006 № 149.

1. **Какие свойства информации являются наиболее важными с точки зрения обеспечения ее безопасности?**

Свойства информации:

* Конфиденциальность – информация недоступна третьим лицам;
* Целостность – информация не искажалась;
* Доступность – к информации есть непрерывный доступ;
* Неотказуемость – авторство информации можно доказать;
* Достоверность – информация соответствует эталонному поведению или состоянию;
* Подотчётность – состояния и жизненный цикл информации или информационной системы можно достоверно отследить;
* Аутентичность – в информацию гарантированно не вносились изменения.
* Ст.3 Федеральный закон «Об информации, информационных технологиях и защите информации».

1. **Охарактеризуйте место правовых мер в системе комплексной защиты информации.**

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

* обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
* соблюдение конфиденциальности информации ограниченного доступа;
* реализацию права на доступ к информации.
* Ст.16 Федерального закона от 27.07.2006 № 149.

1. **Назовите основные цели государства в области обеспечения информационной безопасности.**

Основными целями государства в области обеспечения информационной безопасности являются защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры.

* Об утверждении доктрины информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 05.12.2016 г. № 646.

1. **Перечислите основные нормативные акты РФ, связанные с правовой защитой информации.**

Основные НПА в области защиты информации:

**Федеральные законы:**

* Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
* Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

**Указы Президента РФ:**

* Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;
* Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
* Указ Президента РФ от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации».

1. **Какой закон определяет понятие «официальный документ»?**

Официальные документы – документы, принятые органами государственной власти РФ, другими государственными органами РФ, органами государственной власти субъектов РФ и опубликованные ими или от их имени. Официальные документы удостоверяют события или факты, имеющие юридическое значение и влекущие соответствующие юридические последствия, либо предоставляют права, возлагают обязанности или освобождают от них.

* П.1 ст.5 Федеральный закон от 29.12.1994 77-ФЗ «Об обязательном экземпляре документов».

1. **Какой закон определяет понятие «электронный документ»?**

Электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

* П.11.1 ст.2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1. **В тексте какого закона приведена классификация средств защиты информации?**

* Ст.16 Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 14.07.2022) «Об информации, информационных технологиях и о защите информации».

1. **Какие государственные органы занимаются вопросами обеспечения безопасности информации и какие задачи они решают?**

В соответствии со статьей 8 Федерального закона от 28.12.2010 № 390-ФЗ «О безопасности» Президент РФ устанавливает компетенцию федеральных органов исполнительной власти в области обеспечения безопасности, руководство деятельностью которых он осуществляет и решает в соответствии с законодательством Российской Федерации вопросы, связанные с обеспечением защиты информации и государственной тайны.

Соответствующими указами Президентом определены федеральные органы исполнительной власти, реализующие полномочия по защите информации:

**Федеральная служба то техническому и экспортному контролю Российской Федерации** (ФСТЭК России) – Указ Президента РФ от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

ФСТЭК России является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

* обеспечения безопасности критической информационной инфраструктуры Российской Федерации;
* противодействия иностранным техническим разведкам на территории Российской Федерации;
* обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;
* защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;
* осуществления экспортного контроля.

**Федеральная служба безопасности Российской Федерации** (ФСБ России) - Указ Президента РФ от 11.08.2003 № 960 «Вопросы Федеральной службы безопасности Российской Федерации».

Основными задачами ФСБ России в области защиты информации являются:

* обеспечение в пределах своих полномочий защиты сведений, составляющих государственную тайну, и противодействия иностранным организациям, осуществляющим техническую разведку;
* формирование и реализация в пределах своих полномочий государственной и научно-технической политики в области обеспечения информационной безопасности;
* организация в пределах своих полномочий обеспечения криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и ее учреждениях за рубежом.

1. **Назовите основные положения Доктрины информационной безопасности РФ.**

Основные положения:

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.

2. В настоящей Доктрине на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации.

3. Правовую основу настоящей Доктрины составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, федеральные законы, а также нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации.

4. Настоящая Доктрина является документом стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации, в котором развиваются положения Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 31 декабря 2015 г. № 683, а также других документов стратегического планирования в указанной сфере.

5. Настоящая Доктрина является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности.

* Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

1. **Назовите составляющие правового института государственной тайны.**

Правовой институт государственной тайны имеет три составляющие:

* сведения, относимые к определенному типу тайны (а также принципы и критерии, по которым сведения классифицируются как тайна);
* режим секретности (конфиденциальности) – механизм ограничения доступа к указанным сведениям, т. е. механизм их защиты;
* санкции за неправомерное получение и (или) распространение этих сведений.
* Ст.12 и ст.3 закона РФ от 21.07.1993 № 5485-1 (ред. от 04.08.2022) «О государственной тайне».

1. **В каких случаях нельзя относить информацию к государственной тайне?**

Не подлежат отнесению к государственной тайне и засекречиванию сведения: о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях; о состоянии здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности.

* Ст.7 Закона РФ от 21.07.1993 № 5485-1 (ред. от 04.08.2022) «О государственной тайне».

1. **Какая система обозначения сведений, составляющих государственную тайну, принята в РФ?**

В нашей стране принята следующая система обозначения сведений, составляющих государственную тайну: «особой важности», «совершенно секретно», «секретно».

* Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1.

1. **Назовите группу видов ущерба, возникающего при утечке сведений, составляющих государственную тайну.**

Существуют несколько групп видов ущерба, возникающего при утечке сведений, составляющих государственную тайну: **Политический ущерб; экономический ущерб; моральный ущерб.**

* Ст.283 уголовного кодекса Российской Федерации от 13.06.1996 № 63.

1. **Дайте определение системы защиты государственной тайны и укажите ее составляющие.**

Система защиты государственной тайны - совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.

Государственную тайну составляют:

* сведения в военной области;
* сведения в области экономики, науки и техники;
* сведения в области внешней политики и экономики;
* сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты.
* Ст.2 и ст.5 закона РФ от 21.07.1993 № 5485-1 (ред. от 04.08.2022) «О государственной тайне».

1. **Что в соответствии с законодательством РФ представляет собой засекречивание информации.**

Засекречивание сведений и их носителей – введение для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям. Оно осуществляется в соответствии с принципами законности, обоснованности и своевременности. Определены сведения, не подлежащие засекречиванию (о чрезвычайных происшествиях и катастрофах, о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, преступности и др.).

* Закон РФ от 21.07.1993 № 5485-1 (ред. от 04.08.2022) «О государственной тайне».

1. **Перечислите основные принципы засекречивания информации.**

Отнесение сведений к государственной тайне и их засекречивание осуществляется в соответствии с принципами законности, обоснованности и своевременности.

* Ст.6 закона РФ от 21.07.1993 № 5485-1 (ред. от 04.08.2022) "О государственной тайне".

1. **Что понимается под профессиональной тайной?**

**Профессиональная тайна** – это защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

* Закон РФ от 21.07.1993 № 5485-1 (ред. от 04.08.2022) «О государственной тайне».

1. **Какие виды профессиональных тайн вам известны?**

Профессиональные тайны можно разделить на следующие виды: врачебная, адвокатская, аудиторская, налоговая, таможенная, банковская, нотариальная, страховая, журналистская тайна, исповеди.

* Закон РФ от 21.07.1993 № 5485-1 (ред. от 04.08.2022) «О государственной тайне».

1. **В чем заключается разница между понятием «конфиденциальная информация» и «тайна»?**

Конфиденциальная информация – общее понятие по отношению к коммерческой тайне. Под конфиденциальностью понимают обязательное требование не передавать информацию третьим лицам без согласия владельца.

В отличие от конфиденциальной информации, перечень которой устанавливают по соглашению сторон, коммерческая тайна соответствует условиям, названным в законе:

* она имеет действительную или потенциальную коммерческую ценность в силу неизвестности третьим лицам;
* доступ к ней ограничен на законном основании;
* правообладатель вводит специальный режим коммерческой тайны.

Другими словами, ценность информации, составляющей коммерческую тайну, непосредственно связана с её секретностью. Эта ценность утрачивается, если секрет раскрыт. Конфиденциальная информация, которая не относится к коммерческой тайне, не теряет ценности, если её раскроют. Но владелец несёт убытки, связанные с разглашением этой информации.

* Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149.

1. **В чем состоит сложность служебной тайны с точки зрения определения ее правового режима?**

Исторически служебная тайна не существовала как самостоятельный вид информации ограниченного доступа. Только в 1984 г. было впервые упомянуто в уголовном кодексе понятие «служебная тайна», при этом вводился отдельный состав преступления, предусматривавший ее разглашение иностранной организации (Ст. 76.1. Передача иностранным организациям сведений, составляющих служебную тайну).

В 1987 г. утверждена инструкция1 , которая вводила общее понятие «государственные секреты», в которые включалась государственная тайна (с грифами «особой важности», «совершенно секретно»), служебная тайна (с грифом «секретно») и информация «для служебного пользования». При этом за разглашение информации для служебного пользования предусматривалась только административная ответственность.

Из информации, содержащейся в официально опубликованных документах, можно сделать вывод о том, что сама по себе служебная тайна была механизмом обеспечения нужд государственного управления, которая, с одной стороны, позволяла охранять сведения, распространение которых могло бы повредить системе государственного управления, а с другой стороны, попросту позволяла скрыть огрехи и ошибки политического управления в стране.

В настоящее время регулирование служебной тайны осуществляется не на уровне специального федерального закона, а на уровне преимущественно подзаконных нормативных правовых актов. В силу же Конституции Российской Федерации ограничения конституционных прав, том числе права на информацию, должно осуществляться на уровне федерального закона.

1. **Что представляет собой электронная цифровая подпись?**

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.

* Ст.2 Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 14.07.2022) "Об электронной подписи"

1. **Каковы основные особенности правового режима электронного документа?**

С целью обеспечения правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе, был принят Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи». Его действие распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях. В случае Федерального закона «Об электронной цифровой подписи» определены следующие основные понятия:

* электронный документ – документ, в котором информация представлена в электронно-цифровой форме;
* электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;
* владелец сертификата ключа подписи – физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);
* средства электронной цифровой подписи – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций – создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей;
* сертификат средств электронной цифровой подписи – документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям;
* закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи;
* открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе;
* сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

1. **Назовите основные ограничения на использование электронных документов.**

1. Органы государственной власти, органы местного самоуправления, а также организации, осуществляющие в соответствии с федеральными законами отдельные публичные полномочия, в пределах своих полномочий обязаны предоставлять по выбору граждан (физических лиц) и организаций информацию в форме электронных документов, подписанных усиленной квалифицированной электронной подписью, и (или) документов на бумажном носителе, за исключением случаев, если иной порядок предоставления такой информации установлен федеральными законами или иными нормативными правовыми актами Российской Федерации, регулирующими правоотношения в установленной сфере деятельности.

2. Информация, необходимая для осуществления полномочий органов государственной власти и органов местного самоуправления, организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия, может быть представлена гражданами (физическими лицами) и организациями в органы государственной власти, органы местного самоуправления, в организации, осуществляющие в соответствии с федеральными законами отдельные публичные полномочия, в форме электронных документов, подписанных электронной подписью, если иное не установлено федеральными законами, регулирующими правоотношения в установленной сфере деятельности.

3. Требования к осуществлению взаимодействия в электронной форме граждан (физических лиц) и организаций с органами государственной власти, органами местного самоуправления, с организациями, осуществляющими в соответствии с федеральными законами отдельные публичные полномочия, и порядок такого взаимодействия устанавливаются Правительством Российской Федерации в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

1. **Как называется умышленно искаженная информация?**

Дезинформация-умышленно искаженная информация

* Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149.

1. **Как называется информация, к которой ограничен доступ?**

Конфиденциальная информация – это сведения, доступ к которым ограничен законом, а их разглашение наказуемо.

* Ст.8 Федерального закона от 16.04.2001 № 44.

1. **Какими путями может быть получена информация?**

Анализ имеющихся документов, опросы, интервью и прямое наблюдение.

1. **Как называются компьютерные системы, в которых обеспечивается безопасность информации?**

Компьютерные системы, в которых обеспечивается безопасность информации, называются защищенными.

1. **Основной документ, на основе которого проводится политика информационной безопасности.**

Основным документом, на основе которого проводится политика информационной безопасности, является программа информационной безопасности. Этот документ разрабатывается и принимается как официальный руководящий документ высшими органами управления государством, ведомством, организацией.

1. **В зависимости от формы представления информация может быть разделена на …**

В зависимости от формы представления информация может быть разделена на речевую, телекоммуникационную и документированную. Речевая информация возникает в ходе ведения в помещениях разговоров, работы систем связи, звукоусиления и звуковоспроизведения. Телекоммуникационная информация циркулирует в технических средствах обработки и хранения информации, а также в каналах связи при ее передаче.

1. **К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации?**

К информационным процессам.

* Ст.2 Федерального закона от 10 января 2003 года № 15.

1. **Что называют защитой информации?**

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

* Ст.16 Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 14.07.2022) «Об информации, информационных технологиях и о защите информации».

1. **Под непреднамеренным воздействием на защищаемую информацию понимают?**

Под непреднамеренным воздействием на защищаемую информацию понимают воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий.

* Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149.

1. **Шифрование информации – это?**

Шифрование информации – это преобразование открытой информации в зашифрованную (которая чаще всего называется шифр-текстом или криптограммой), и наоборот. Первая часть этого процесса называется зашифрованием, вторая - расшифрованием.

1. **Основные предметные направления защиты информации?**

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

* обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
* соблюдение конфиденциальности информации ограниченного доступа;
* реализацию права на доступ к информации.
* Ст.16 федерального закона от 27.07.2006 № 149-ФЗ (ред. от 14.07.2022) «Об информации, информационных технологиях и о защите информации».

1. **Государственная тайна – это?**

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

* Ст.2 закона РФ от 21.07.1993 № 5485-1 (ред. от 04.08.2022) «О государственной тайне».

1. **Коммерческая тайна – это?**

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.

* Ст.3 Федерального закона от 29.07.2004 № 98-ФЗ (ред. от 14.07.2022) «О коммерческой тайне».

1. **Банковская тайна – это?**

Банковская тайна – это запрет кредитным учреждениям разглашать информацию о своих клиентах, их счетах и операциях. Исключение может быть сделано только в интересах государства или правосудия.

* Ст.857 ГК РФ

1. **Профессиональная тайна – это?**

Профессиональная тайна – это защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

1. **К основным объектам банковской тайны относятся следующие:**

К банковской тайне относятся:

* данные о состоянии счетов клиентов;
* операции, проведенные по поручению клиента;
* финансовое положение клиентов;
* системы охраны банка и клиентов;
* информация о структуре юридического лица - клиента, о руководителях, видах деятельности;
* данные о коммерческой деятельности клиентов;
* сведения об отчетности по банку, за исключением подлежащей опубликованию;
* коды защиты информации, а также другие данные, перечень которых может устанавливать финансовое учреждение.

1. **Как называется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений?**

Право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений – основные конституционные права и свободы человека и гражданина.

* Федеральный закон от 07.07.2003 № 126.

1. **Как называются сведения, доверенные нотариусу в связи с совершением нотариальных действий?**

Сведения, доверенные нотариусу в связи с совершением нотариальных действий, называются нотариальной тайной.

* Ст.5 «Основы законодательства Российской Федерации о нотариате» (утв. ВС РФ 11.02.1993 № 4462-1).

1. **Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право …**

Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе, может быть осуществлен только тем лицам, которые на это имеют право называется функцией защиты коммерческой тайны.

1. **Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем …**

Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем – защита от сбоев серверов, рабочих станций и локальных компьютеров.

* Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149.

1. **Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных …**

Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных называется – защита от сбоев устройств для хранения информации.

1. **Технические каналы утечки информации делятся на …**

Технические каналы утечки информации делятся на каналы:

* по физической природе носителя;
* по информативности;
* по времени функционирования;
* по структуре.

1. **Можно выделить следующие направления мер информационной безопасности …**

Можно выделить следующие направления мер информационной безопасности:

* Правовые;
* Организационные;
* Технические.

1. **Что можно отнести к правовым мерам ИБ?**

К правовым мерам обеспечения информационной безопасности относятся:

* разработка норм, устанавливающих ответственность за компьютерные преступления;
* защита авторских прав программистов;
* совершенствование уголовного и гражданского законодательства

совершенствование судопроизводства;

* общественный контроль разработчиков компьютерных систем;
* принятие соответствующих международных соглашений.

1. **Что можно отнести к организационным мерам ИБ?**

Организационные меры защиты – меры организационного характера, предназначенные для регламентации функционирования информационных систем, работы персонала, взаимодействия пользователей с системой. Среди базовых организационных мер по защите информации можно выделить следующее:

* Формирование политики безопасности;
* Регламентация доступа в помещения;
* Регламентация допуска сотрудников к использованию ресурсов информационной системы и др;
* Определение ответственности в случае несоблюдения требований информационной безопасности.

1. **Что можно отнести к техническим мерам ИБ?**

С помощью технических средств защиты информации решаются следующие задачи:

Создание физических (механических) препятствий на пути проникновения к носителям информации (решетки, сейфы, бронированные двери и стекла, замки и др.).

Выявление попыток проникновения на объект охраны, к местам сосредоточения носителей защищаемой информации (средства охранной сигнализации).

Предупреждение о возникновении чрезвычайных ситуаций (пожар, наводнение и т.п.) и их ликвидация (пожарная сигнализация, средства пожаротушения, средства оповещения и т.п.).

Поддержание связи с различными организациями, подразделениями, помещениями и другими объектами охраны (радио- и проводные средства связи, сигнальные устройства и т.п.).

Нейтрализация, поглощение или отражение излучения используемых радио-технических устройств (экраны, защитные фильтры, разделительные устройства в сетях электроснабжения, средства электромагнитного зашумления и т.п.).

Введение технических разведок в заблуждение (дезинформация) относительно истинного содержания защищаемой информации.

Комплексная проверка режимных помещений, использующихся каналов связи и средств обработки информации на соответствие требованиям безопасности информации, профилактические мероприятия по защите использующейся там информации (средства акустического зашумления помещений, "прожигатели" телефонных подслушивающих устройств, индикаторы электромагнитных излучений, программно-аппаратные средства контроля радиоэфира и т.п.).

Комплексная защита информации в автоматизированных системах обработки данных с помощью фильтров, электронных замков и ключей, систем разграничения доступа к защищаемой информации в целях предотвращения ее несанкционированного копирования, искажения или изменения.