**Методические указания**

**по выполнению практических работ по дисциплине**

**«Нормативные документы и стандарты по информационной безопасности»**

Казань – 2021

**ПРАКТИЧЕСКАЯ РАБОТА № 1**

**(практические занятия № 1 - № 5)**

**по дисциплине «Международные и российские нормативные правовые акты, стандарты в области обеспечения информационной безопасности»**

**Тема:** Структура и содержание международных и российских нормативных правовых актов, стандартов в области обеспечения информационной безопасности.

**Содержание и методика выполнения заданий:**

Для выполнения задания необходимо ознакомиться с содержанием международных и российских нормативных правовых актов, размещенных на официальных сайтах ФСТЭК России (<https://fstec.ru/>), ФСБ России (<http://www.fsb.ru/>) и Роскомнадзора (<https://rkn.gov.ru/>), а также в справочной правовой системе КонсультантПлюс (<http://www.consultant.ru/>) или в системе «Гарант» (<https://www.garant.ru/>). Получив представление о содержании различных видов нормативных правовых актов, обучающиеся выполняют следующие виды заданий:

**Задание 1.** В виде схемы представить структуру международных и российских нормативных правовых актов, стандартов в области обеспечения информационной безопасности: Конституция, ФКЗ, Кодексы, ФЗ, Указы Президента РФ, Постановления Правительства РФ, НПА ФОИВ РФ, Стандарты, Международные НПА, НПА субъектов РФ, ГОСТы, Прочее (Приложение 1).

**Время: 5 час.**

**Задание 2.** По результатам изучения основных положений международных и российских нормативных правовых актов, стандартов в области обеспечения информационной безопасности (с учетом внесенных в них изменений на дату оформления отчета по практической работе) необходимо заполнить разделы Отчета по практической работе (Приложение 1, Приложение 2).

**Время: 5 час.**

**Отчет**

**по практической работе № 1**

**(практические занятия № 1 - № 5)**

**Тема:** Анализ международных и российских нормативных правовых актов, стандартов в области обеспечения информационной безопасности.

**Цель занятия** – изучить современное состояние нормативно-правовой базы в области обеспечения информационной безопасности.

**Выполнил**

Обучающийся группы \_\_\_\_\_\_\_\_\_

Фамилия Имя Отчество \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Содержание и методика выполнения заданий:**

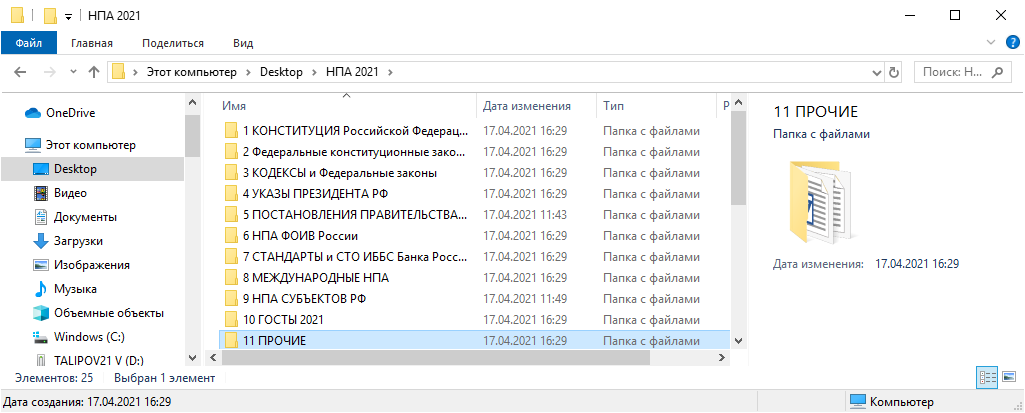
Для выполнения задания необходимо ознакомиться с содержанием международных и российских нормативных правовых актов, размещенных на официальных сайтах ФСТЭК России (<https://fstec.ru/>), ФСБ России (<http://www.fsb.ru/>) и Роскомнадзора (<https://rkn.gov.ru/>), а также в справочной правовой системе КонсультантПлюс (<http://www.consultant.ru/>) или в системе «Гарант» (<https://www.garant.ru/>). Получив представление о содержании различных видов нормативных правовых актов, обучающиеся выполняют следующие виды заданий:

**Задание 1.** В виде схемы представить структуру международных и российских нормативных правовых актов, стандартов в области обеспечения информационной безопасности: Конституция, ФКЗ, Кодексы, ФЗ, Указы Президента РФ, Постановления Правительства РФ, НПА ФОИВ РФ, Стандарты, Международные НПА, НПА субъектов РФ, ГОСТы, Прочее (Приложение 1).

**Задание 2.** По результатам изучения основных положений международных и российских нормативных правовых актов, стандартов в области обеспечения информационной безопасности (с учетом внесенных в них изменений на дату оформления отчета по практической работе) необходимо заполнить разделы Отчета по практической работе (Приложение 1, Приложение 2).

**Приложение 1**

**1. Примеры наименований папок с файлами НПА (Скриншот)**



**2. Наименование (Содержание) папок с файлами НПА (Скриншот)**

1 КОНСТИТУЦИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

2 ФЕДЕРАЛЬНЫЕ КОНСТИТУЦИОННЫЕ ЗАКОНЫ

3 КОДЕКСЫ и ФЕДЕРАЛЬНЫЕ ЗАКОНЫ

4 УКАЗЫ ПРЕЗИДЕНТА РФ

5 ПОСТАНОВЛЕНИЯ ПРАВИТЕЛЬСТВА РФ

6 НПА ФОИВ РОССИИ

7 СТАНДАРТЫ и СТО ИББС БАНКА РОССИИ

8 МЕЖДУНАРОДНЫЕ НПА

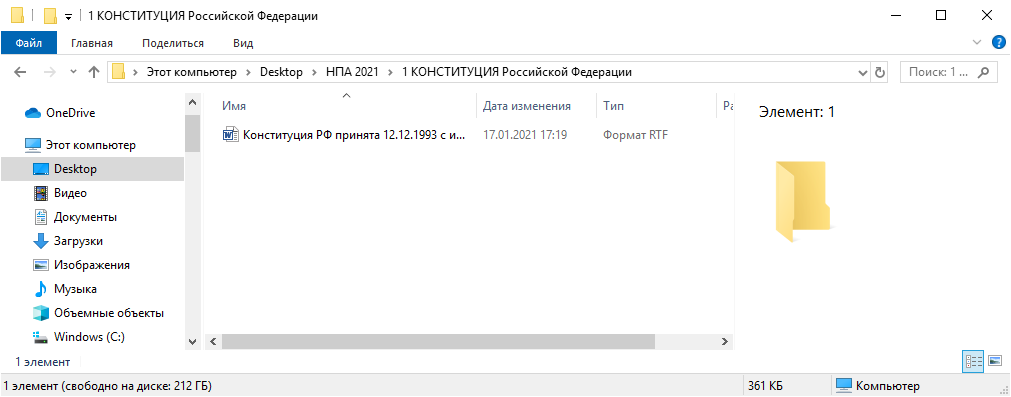
9 НПА СУБЪЕКТОВ РФ

10 ГОСТЫ

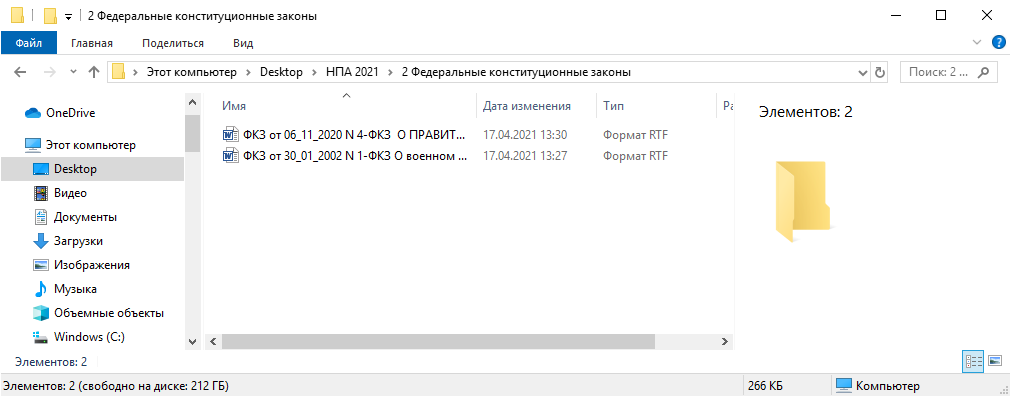
11 ПРОЧЕЕ

**3. Содержание папок с файлами НПА (Скриншоты):**

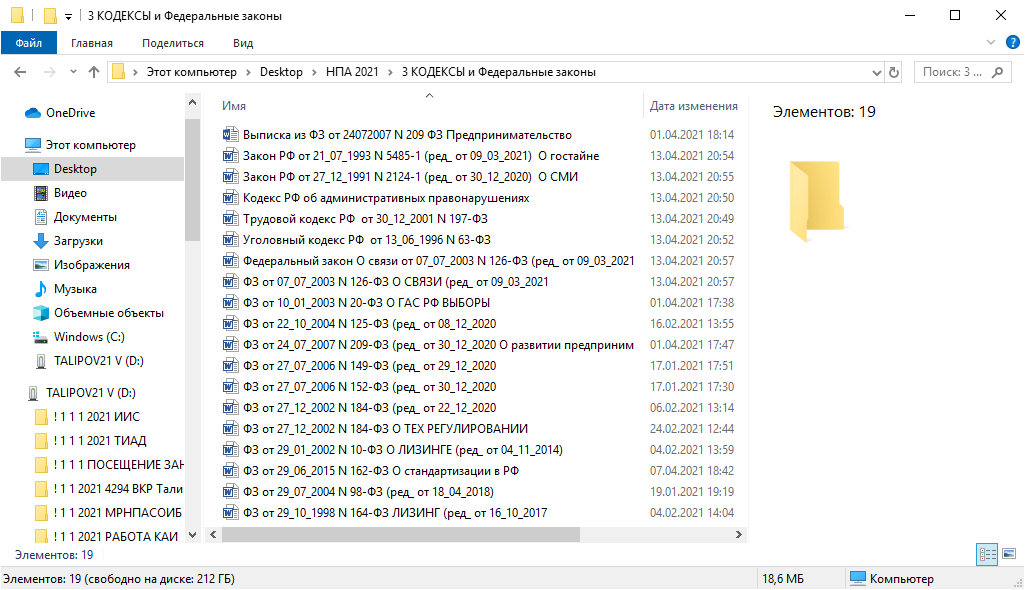
**1 КОНСТИТУЦИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**



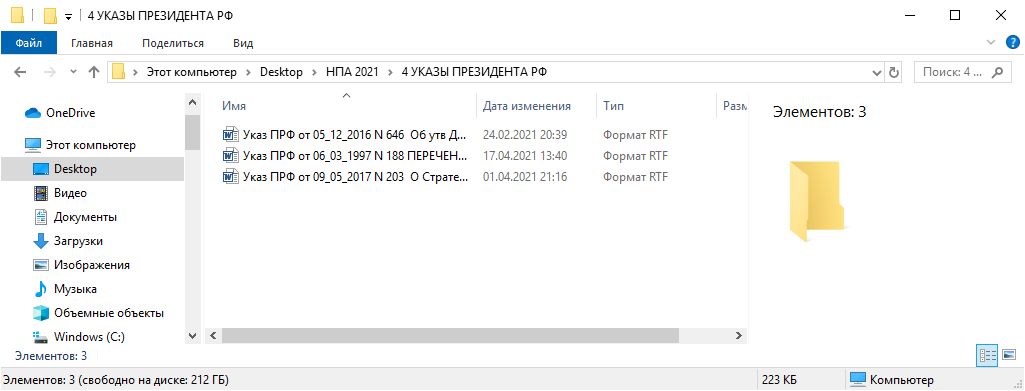
**2 ФЕДЕРАЛЬНЫЕ КОНСТИТУЦИОННЫЕ ЗАКОНЫ**



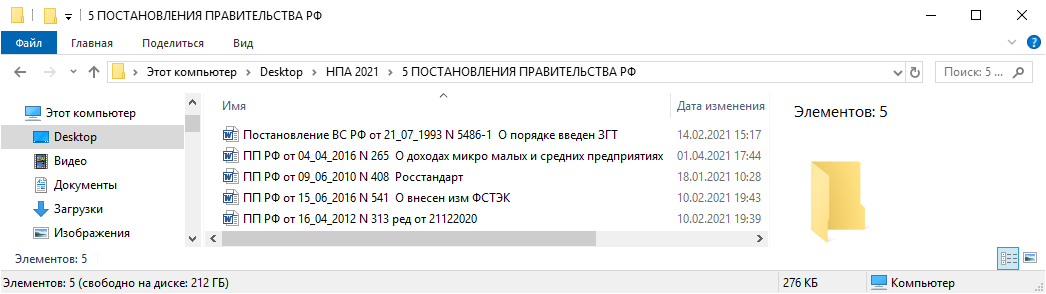
**3 КОДЕКСЫ и ФЕДЕРАЛЬНЫЕ ЗАКОНЫ**



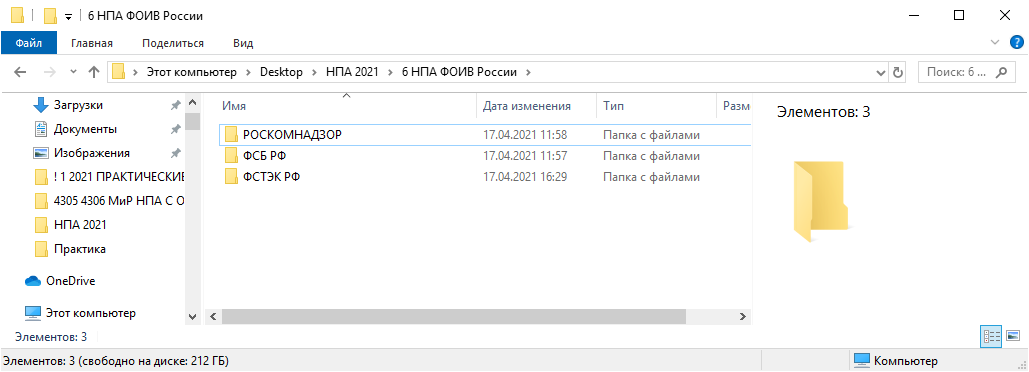
**4 УКАЗЫ ПРЕЗИДЕНТА РФ**

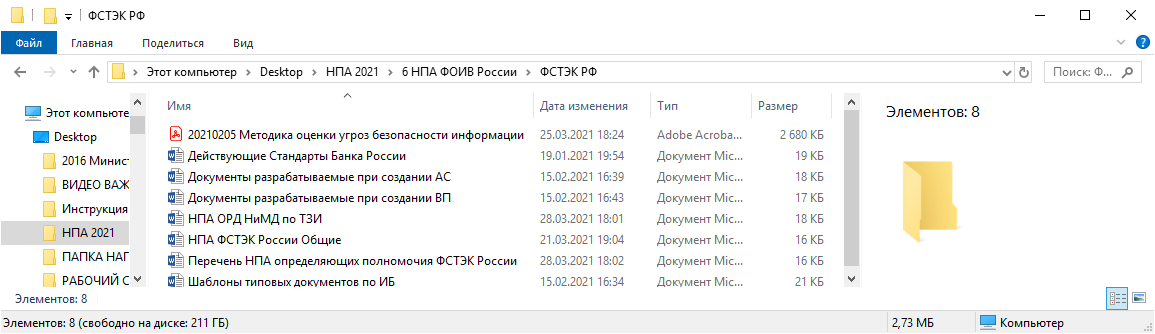


**5 ПОСТАНОВЛЕНИЯ ПРАВИТЕЛЬСТВА РФ**

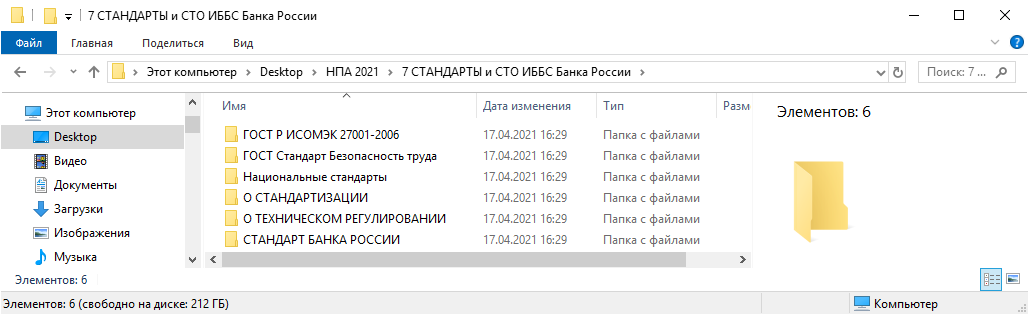


**6 НПА ФОИВ РФ**

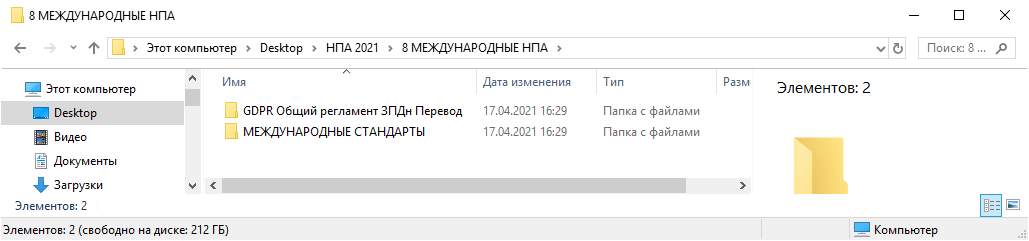




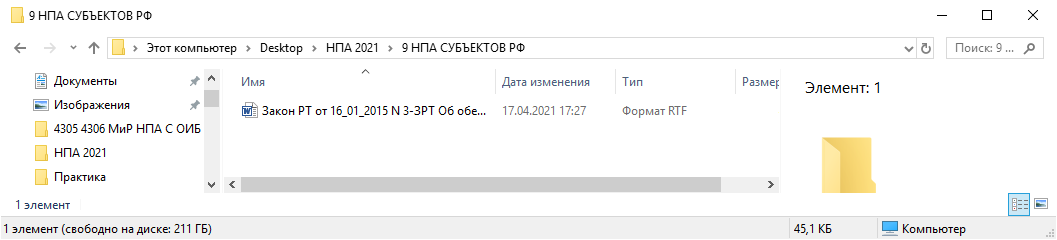
**7 СТАНДАРТЫ и СТО ИББС БАНКА РОССИИ**



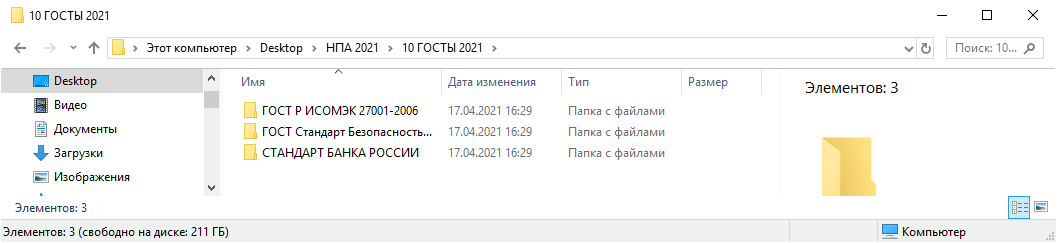
**8 МЕЖДУНАРОДНЫЕ НПА**



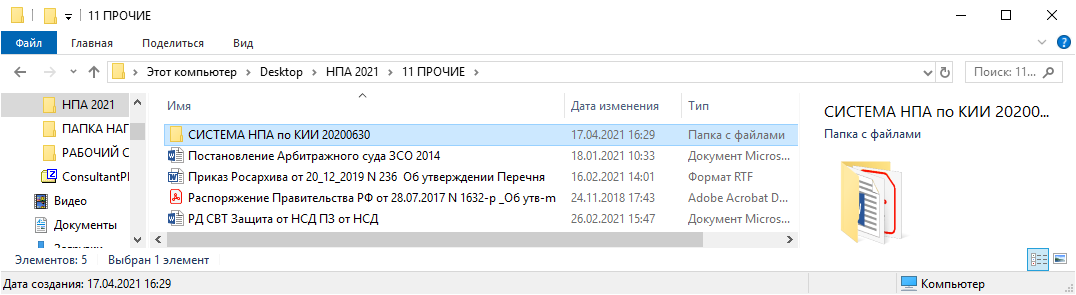
**9 НПА СУБЪЕКТОВ РФ**



**10 ГОСТЫ**



**11 ПРОЧЕЕ**



**Приложение 2**

**Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации**

<https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty>

<https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii>

**Законы: 3**

**Указы: 5**

**Постановления: 1**

**Приказы: 7**

**Положения: 1**

**Специальные нормативные документы: 12**

**Национальные стандарты: 1**

**Проекты: 1**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Законы (3):**

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

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

3. Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне».

**Указы (5):**

1. Указ Президента Российской Федерации от 25.11.2017 № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16.08.2004 № 1085».

2. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

3. Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

4. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера».

5. Указ Президента Российской Федерации от 30.11.1995 № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне».

**Постановления (1):**

1. Постановление Правительства РФ от 25.08.2005 № 537 «О функциях федеральных органов исполнительной власти, Государственной корпорации по атомной энергии «Росатом» и Российской академии наук по реализации договора о всеобъемлющем запрещении ядерных испытаний».

**Приказы (7):**

1. Приказ ФСТЭК России от 23.03.2017 № 49 «О внесении изменений в Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21, и в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14.03.2014 № 31».

2. Приказ ФСТЭК России от 15.02.2017 № 27 «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17».

3. Совместный приказ ФСТЭК России, ФСБ России и Минкомсвязи России от 31.12.2013 № 151/786/461 «О признании утратившим силу приказа Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

4. 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».

5. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

6. Приказ ФСТЭК России от 31.08.2010 № 489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования».

7. Решение ФСТЭК России от 05.03.2010 «Не применять методические документы: Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утвержденные заместителем директора ФСТЭК России 15 февраля 2008 г.; Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные заместителем директора ФСТЭК России 15 февраля 2008 г.».

**Положения (1):**

1. Положение от 25 ноября 1994 г. «По аттестации объектов информатизации по требованиям безопасности информации».

**Специальные нормативные документы (12):**

1. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г. «Методика оценки угроз безопасности информации».

2. Методический документ. Утвержден ФСТЭК России 26 июня 2018 г. «Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в Банк данных угроз безопасности информации ФСТЭК России».

3. Методический документ. Утвержден ФСТЭК России 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год «При рассмотрении угроз утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН) необходимо применять полную версию данного документа».

5. Методический документ. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год («Методика оценки угроз безопасности информации». Пометка «для служебного пользования» снята Решением ФСТЭК России от 16 ноября 2009 г.).

6. Руководящий документ. Приказ председателя Гостехкомиссии России от 19.06.2002 № 187 «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий».

7. Руководящий документ. Приказ председателя Гостехкомиссии России от 04.06.1999 № 114 «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».

8. Руководящий документ. Решение председателя Гостехкомиссии России от 25 июля 1997 г. «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации».

9. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

10. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

11. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. «Защита от несанкционированного доступа к информации. Термины и определения».

12. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».

**Национальные стандарты (1):**

1. Настоящие стандарты не могут быть полностью или частично воспроизведены, тиражированы и распространены в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

<https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii>

**Проекты (1):**

1. Методический документ. Методика моделирования угроз безопасности информации.

<https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii>

**ПРАКТИЧЕСКАЯ РАБОТА № 2  
(практические занятия № 6 - № 9)**

**по дисциплине «Международные и российские нормативные правовые акты, стандарты в области обеспечения информационной безопасности»**

**Тема:** Правонарушения в информационной сфере.

**Цель занятия** – изучить современное состояние нормативно-правовой базы в области обеспечения информационной безопасности.

**Содержание и методика выполнения заданий:**

Для выполнения задания необходимо ознакомиться с содержанием международных и российских нормативных правовых актов, размещенных на официальных сайтах ФСТЭК России (<https://fstec.ru/>), ФСБ России (<http://www.fsb.ru/>) и Роскомнадзора (<https://rkn.gov.ru/>), а также в справочной правовой системе КонсультантПлюс (<http://www.consultant.ru/>) или в системе «Гарант» (<https://www.garant.ru/>). Получив представление о содержании различных видов нормативных правовых актов, обучающиеся выполняют следующие виды заданий:

**Задание 1.** В виде схемы представить структуру международных и российских нормативных правовых актов, стандартов в области обеспечения информационной безопасности: Конституция, ФКЗ, Кодексы, ФЗ, Указы Президента РФ, Постановления Правительства РФ, НПА ФОИВ РФ, Стандарты, Международные НПА, НПА субъектов РФ, ГОСТы, Прочее (Приложение 1).

**Время: 4 час.**

**Задание 2.** По результатам изучения основных положений международных и российских нормативных правовых актов в области обеспечения информационной безопасности необходимо провести анализ видов правонарушений и перечислить предусмотренные виды наказаний за совершенные правонарушения (преступления) в информационной сфере (Приложение 2).

**Время: 4 час.**

**Отчет по практической работе № 2  
(практические занятия № 6 - № 9)**

**Тема:** Правонарушения в информационной сфере.

**Цель занятия** – изучить современное состояние нормативно-правовой базы в области обеспечения информационной безопасности.

**Выполнил**

Обучающийся группы \_\_\_\_\_\_\_\_\_\_\_

Фамилия Имя Отчество \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Содержание и методика выполнения заданий:**

Для выполнения задания необходимо ознакомиться с содержанием международных и российских нормативных правовых актов, размещенных на официальных сайтах ФСТЭК России (<https://fstec.ru/>), ФСБ России (<http://www.fsb.ru/>) и Роскомнадзора (<https://rkn.gov.ru/>), а также в справочной правовой системе КонсультантПлюс (<http://www.consultant.ru/>) или в системе «Гарант» (<https://www.garant.ru/>). Получив представление о содержании различных видов нормативных правовых актов, обучающиеся выполняют следующие виды заданий:

**Задание 1.** Представить Перечень международных и российских нормативных правовых актов, предусматривающих ответственность за правонарушения в области информационной безопасности (защиты информации): Конституция, ФКЗ, Кодексы, ФЗ, Указы Президента РФ, Постановления Правительства РФ, НПА ФОИВ РФ, Международные НПА, НПА субъектов РФ (Приложение 1).

**Задание 2.** По результатам изучения основных положений международных и российских нормативных правовых актов в области обеспечения информационной безопасности необходимо провести анализ видов правонарушений и перечислить предусмотренные виды наказаний за совершенные правонарушения (преступления) в информационной сфере (Приложение 2).

**Отчет по практической работе № 2**

**Тема: Правонарушения в информационной сфере**

**Приложение 1**

**Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации**

<https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty>

<https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii>

**Законы: 3**

**Указы: 5**

**Постановления: 1**

**Приказы: 7**

**Положения: 1**

**Специальные нормативные документы: 12**

**Национальные стандарты: 1**

**Проекты: 1**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Законы (3):**

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

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

3. Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне».

**Указы (5):**

1. Указ Президента Российской Федерации от 25.11.2017 № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16.08.2004 № 1085».

2. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

3. Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

4. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера».

5. Указ Президента Российской Федерации от 30.11.1995 № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне».

**Постановления (1):**

1. Постановление Правительства РФ от 25.08.2005 № 537 «О функциях федеральных органов исполнительной власти, Государственной корпорации по атомной энергии «Росатом» и Российской академии наук по реализации договора о всеобъемлющем запрещении ядерных испытаний».

**Приказы (7):**

1. Приказ ФСТЭК России от 23.03.2017 № 49 «О внесении изменений в Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21, и в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14.03.2014 № 31».

2. Приказ ФСТЭК России от 15.02.2017 № 27 «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17».

3. Совместный приказ ФСТЭК России, ФСБ России и Минкомсвязи России от 31.12.2013 № 151/786/461 «О признании утратившим силу приказа Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

4. 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».

5. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

6. Приказ ФСТЭК России от 31.08.2010 № 489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования».

7. Решение ФСТЭК России от 05.03.2010 «Не применять методические документы: Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утвержденные заместителем директора ФСТЭК России 15 февраля 2008 г.; Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные заместителем директора ФСТЭК России 15 февраля 2008 г.».

**Положения (1):**

1. Положение от 25 ноября 1994 г. «По аттестации объектов информатизации по требованиям безопасности информации».

**Специальные нормативные документы (12):**

1. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г. «Методика оценки угроз безопасности информации».

2. Методический документ. Утвержден ФСТЭК России 26 июня 2018 г. «Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в Банк данных угроз безопасности информации ФСТЭК России».

3. Методический документ. Утвержден ФСТЭК России 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год «При рассмотрении угроз утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН) необходимо применять полную версию данного документа».

5. Методический документ. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год («Методика оценки угроз безопасности информации». Пометка «для служебного пользования» снята Решением ФСТЭК России от 16 ноября 2009 г.).

6. Руководящий документ. Приказ председателя Гостехкомиссии России от 19.06.2002 № 187 «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий».

7. Руководящий документ. Приказ председателя Гостехкомиссии России от 04.06.1999 № 114 «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».

8. Руководящий документ. Решение председателя Гостехкомиссии России от 25 июля 1997 г. «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации».

9. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

10. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

11. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. «Защита от несанкционированного доступа к информации. Термины и определения».

12. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».

**Национальные стандарты (1):**

1. Настоящие стандарты не могут быть полностью или частично воспроизведены, тиражированы и распространены в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

<https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii>

**Проекты (1):**

1. Методический документ. Методика моделирования угроз безопасности информации.

<https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii>

**Приложение 2**

**Тема: Правонарушения в информационной сфере**

**Цель занятия** – Провести анализ правонарушений в информационной сфере, перечислить предусмотренные виды наказаний за совершенные правонарушения в информационной сфере.

* **Зелёный цвет** - ***без изменений***
* **Красный цвет - *утратило силу***
* **Бирюзовый цвет - *добавлено***

**Правонарушения в информационной сфере**

Правонарушения в информационной сфере делятся на проступки (деликты) и преступления. Под правонарушением обычно понимается противоправное виновное нарушение субъектом действующей нормы информационного права, в результате чего наносится существенный вред интересам личности, государства, общества в информационной сфере.

Все правонарушения выступают в качестве юридических фактов, причем эти действия или бездействие субъектов могут повлечь для последних неблагоприятные последствия личного, организационного, имущественного характера, вытекающие из санкции нарушенной информационно-правовой нормы в определенном регламентированном порядке.

Наиболее распространенными правонарушениями в информационной сфере являются проступки, имеющие следующие особенности:

— они отличаются незначительной опасностью (вред для общества);

— совершаются в различных областях информационной деятельности;

— направлены на различные объекты и имеют разные юридические последствия.

Проступки подразделяются на дисциплинарные, административные и деликты.

Дисциплинарные проступки в информационной сфере — это правонарушения, совершаемые субъектами информационного права в связи с неисполнением или ненадлежащим исполнением возложенных на них трудовых обязанностей, влекущие за собой применение дисциплинарного или общественного воздействия, предусмотренного трудовым законодательством. К совершившему дисциплинарный проступок должностному лицу или гражданину применяются различные меры наказания: замечание, выговор, увольнение по соответствующим основаниям, а также иные взыскания в соответствии с уставами и положениями о дисциплине (ч. 5 ст. 189, ст. 192 ТК РФ) для отдельных категорий работников. ***(изменений не претерпел)***

Административным проступком в информационной сфере называется противоправное, виновное (умышленное или неосторожное) действие либо бездействие физического или юридического лица, посягающее на информационные права и свободы человека и гражданина, здоровье, общественную нравственность, установленный порядок осуществления государственной власти, общественный порядок и общественную безопасность, собственность, законные интересы других лиц, за которое законодательством предусмотрена административная ответственность. В соответствии со ст. 3.2. КоАП РФ это: предупреждение; административный штраф; возмездное изъятие орудия совершения или предмета административного правонарушения; ***(данный пункт статьи 3.2 КоАП РФ утратил силу в соответствии с Федеральным законом от 28.12.2010 № 398-ФЗ)***конфискация орудия совершения или предмета административного правонарушения; лишение специального права, предоставленного физическому лицу; административный арест; административное выдворение за пределы страны иностранного гражданина или лица без гражданства; дисквалификация; административное приостановление деятельности; обязательные работы ***(Пункт введен - Федеральный закон от 08.06.2012 № 65-ФЗ)***; административный запрет на посещение мест проведения официальных спортивных соревнований в дни их проведения ***(Пункт введен - Федеральный закон от 23.07.2013 № 192-ФЗ).***

Действующий КоАП РФ включает информационные правонарушения в разные главы (например, гл. 5-8, 13-17, 19), однако в нем есть и специальная гл. 13 «Административные правонарушения в области связи и информации» (ст. 13.2-13.46; ст. 13.1 утратила силу). Согласно ст. 2.1 КоАП РФ административная ответственность, в частности за нарушение информационного законодательства, может быть установлена как федеральным законодательством, так и законодательством субъектов РФ.

Деликтами называются правонарушения, выражающиеся в нарушении норм, регулирующих информационно-имущественные отношения организаций, физических лиц, предпринимательских структур. Их называют также гражданскими правонарушениями. В суде могут быть предъявлены претензии к гражданам, организациям, ведомствам и др., и они обязаны возместить причиненный ущерб или убытки либо восстановить нарушенные информационные права.

Наиболее серьезными правонарушениями в информационной сфере являются преступления; к лицам, их совершившим, судом применяются меры уголовного наказания: лишение свободы, права занимать определенные должности, арест, штраф и др. Например, за оскорбление, содержащееся в публичном выступлении, публично демонстрирующемся произведении или СМИ (ст. 130 УК РФ).

Анализ показал, что всем указанным правонарушениям присущи определенные юридически значимые признаки (противоправность, общественная опасность, виновность и возможная наказуемость), среди которых наиболее важным в информационной сфере является противоправность, выраженная в том, что противоправным правонарушением в рассматриваемой области может быть лишь деяние, запрещенное нормой информационного права.

Общественная опасность представляет собой исходный материальный признак любого правонарушения, позволяющий отличить одно правонарушение в информационной сфере от другого (например, административный проступок от преступления в сфере компьютерной информации). Данный признак выражает объективное свойство рассматриваемого правонарушения, которое означает способность причинить определенный вред информационно-правовым отношениям, охраняемым информационным или иным законодательством, под защитой и охраной которого находятся наиболее важные информационные права и свободы граждан, интеллектуальная собственность, права журналистов, СМИ, архивы, безопасность страны, государственные секреты и др. Другие информационные явления только предстоит урегулировать с точки зрения права.

Еще одним признаком правонарушения в информационной сфере является его виновность, непосредственно вытекающая из понятия вины и выражающаяся в двух формах: в форме умысла (например, умышленное оскорбление журналиста на пресс-конференции должностным лицом) и неосторожности (в частности, легкомысленная или небрежная передача служебных материалов иностранцу). Однако если правонарушение в информационной сфере совершено без вины (случайно) и не влечет негативных последствий, то оно может и не рассматриваться как правонарушение и соответственно лицо, его совершившее, не привлекается к ответственности.

Четвертым признаком правонарушения является возможная наказуемость, связанная с предыдущими признаками и свидетельствующая о наступлении юридически значимых последствий после совершения лицом информационного правонарушения. Под наказуемостью не следует понимать автоматическое наказание после совершения правонарушения в исследуемой области; она предполагает лишь возможность применения наказания за определенное противоправное действие, предусмотренное нормой информационного права. Например, сообщение программистом при приеме на работу ложных сведений о себе и о своей прежней деятельности может послужить основанием для отказа в его допуске

к государственной тайне и принятии иных мер (ст. 22 Закона РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне»). (абзац шестой части первой статьи 22 изменений не претерпел)

Состав правонарушения в информационной сфере — *это совокупность характерных признаков рассматриваемого правонарушения, которые предусмотрены соответствующими нормами информационного права и характеризуют данное правонарушение как общественно опасное, противоправное и наказуемое явление.*

Все признаки, характеризующие состав правонарушения в исследуемой области, существуют не отдельно, а в связи друг с другом. Они группируются в нечто целое, содержащее в себе четыре основных элемента: субъект правонарушения в данной области и субъективная сторона, объект правонарушения в информационной среде и объективная сторона.

Субъект правонарушения в информационной сфере — *это конкретное лицо (лица), которое совершило противоправные действия и должно за это нести ответственность в установленном законом порядке.* К субъектам могут относиться разные лица: граждане, авторы программных продуктов, журналисты, редакторы, работники информационных телерадиокомпаний и служб, изобретатели, госслужащие, предприниматели, судьи, следователи и многие другие. Это должны быть физически вменяемые люди, достигшие определенного возраста, с которого наступает ответственность по действующему законодательству, причем юридические лица привлекаются к административной и гражданско-правовой ответственности. Можно выделить также субъекты, несущие специальную редакционную ответственность (главные редакторы традиционных и сетевых СМИ и т.д.).

Субъективную сторону правонарушения характеризует *психическое отношение субъекта преступления к совершенному противоправному действию или бездействию в области информации, информатизации и иных информационных областях.* При анализе этого элемента, который может осуществляться и в отношении положительных информационных действий субъектов, рассматриваются такие юридические и психологические признаки, как цель и задачи противоправных информационных действий, их мотив, желание, форма вины и т.д. Для характеристики субъективной стороны имеют значение две формы вины: умышленная или неосторожная. В связи с этим для органов следствия важно установить, как совершено правонарушение в информационной сфере: умышленно или по неосторожности.

Объект правонарушения включает *информационно-правовые, а также тесно связанные с ними отношения, которые охраняются действующим информационным законодательством и которым конкретным правонарушением приносится общественный ущерб или создается угроза причинения ущерба.* К непосредственным объектам правонарушения в информационной сфере относятся самые разные явления — сама информация, информационные ресурсы, печатная продукция, архивные документы, программы для ЭВМ и баз данных, топологии интегральных микросхем, сами ЭВМ, их сети и многое другое.

Информационные правонарушения по объекту посягательств можно разделить на четыре группы:

— противоправные посягательства в сфере реализации информационных прав и свобод человека и гражданина (нарушение права доступа к открытой, массовой информации; нарушение тайны переписки; злоупотребление свободой слова, свободой массовой информации);

— противоправные посягательства в сфере организации и деятельности СМИ (введение цензуры; воспрепятствование профессиональной работе журналиста и др.);

— противоправные посягательства против мер, обеспечивающих информационную безопасность общества, государства, гражданина (посягательства против защиты государственной тайны; нарушение правил сертификации телекоммуникационного оборудования; умышленное уничтожение государственных информационных ресурсов; искажение (непредставление) экологической информации, в результате чего наносится ущерб здоровью населения и функционированию экосистем, и др.);

— противоправные посягательства против индустрии телекоммуникаций и связи (несанкционированный доступ к компьютерной информации; распространение вредоносных программ; распространение детской порнографии в Сети; мошенничество с использованием информационных технологий; подлог информации; незаконный перехват информации и др.).

Объективная сторона правонарушения в информационной сфере проявляется во внешней стороне этого негативного явления, т.е. *выражается прежде всего в том, как субъект воспринял данное проявление, что видел, слышал и т.д.* При этом важно проанализировать само негативное информационное действие либо бездействие, наступившие в результате последствия, причинную связь между ними, место, время совершения неправомерных актов, условие, орудие, способы и др. Объективная сторона может характеризовать и положительные информационно-правовые акты, явления и процессы. Она содержит ряд элементов: поведение правонарушителя, место и время совершения правонарушения, причем информационные правонарушения включают в себя как действие, так и бездействие, выразившееся, например, в непринятии определенных мер по защите информации, а также противоправное превышение или неприменение своих полномочий.

Для иллюстрации охарактеризуем некоторые составы правонарушений в информационной сфере, основываясь на приведенных выше определениях и действующем российском законодательстве.

1. Законодательство о связи и информационных технологиях. Нарушение тайны связи (ст. 63 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»). ***(изменений не претерпел)***

Объект данного правонарушения - охраняемые информационным законодательством общественные отношения в сфере тайны переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи.

Объективную сторону рассматриваемого правонарушения образует совокупность самостоятельных информационно-правовых действий: подслушивание телефонных переговоров, неправомерное ознакомление с сообщениями электросвязи, задержка, осмотр и выемка почтовых отправлений и документальной корреспонденции, получение сведений о них, а также иные ограничения связи.

Субъективная сторона этого негативного проявления выражается в форме умысла. Лицо сознает, что своими незаконными действиями нарушает закон и права граждан, сознательно идет на это (возможно, и по указанию вышестоящих органов) и тем самым совершает серьезное правонарушение.

Субъекты данного правонарушения — операторы связи, должностные лица и иные работники организаций связи. В статье сказано, что лица, допустившие указанные выше нарушения, привлекаются к ответственности, установленной законодательством РФ (санкция неконкретная, отсылочная).

2. Законодательство о СМИ. Ответственность за ущемление свободы массовой информации (ст. 38 Закона РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации»). Объект правонарушения — охраняемая законом правомерная деятельность СМИ, а также журналистов, издателей, распространителей печатной продукции, режиссеров, ведущих телепрограмм и др.

Объективная сторона правонарушения образует здесь два противоправных действия в информационной сфере:

а) воспрепятствование в какой бы то ни было форме со стороны различных субъектов законной деятельности СМИ, журналистов и иных лиц;

б) обнаружение органов, *органов местного самоуправления,* организаций, учреждений или должностей, в задачи которых входит осуществление цензуры СМИ.

Субъективная сторона правонарушения — вина в форме прямого умысла. Соответствующие лица, работники, органы, органы местного самоуправления и т.д. осознают, что, препятствуя работе СМИ, нарушают указанный закон и, вводя цензуру, предвидят возможность наступления негативных последствий, но, несмотря на это, действуют вопреки закону.

В качестве субъекта данного правонарушения выступают разные лица, руководители, служащие; их действия влекут за собой уголовную, административную, дисциплинарную и иную ответственность (санкция неконкретная, отсылочная).

Предоставление государственными органами, органами местного самоуправления информации о своей деятельности по запросам редакций, если такие отношения не урегулированы законодательством Российской Федерации о средствах массовой информации, осуществляется в соответствии с законодательством Российской Федерации, регулирующим вопросы обеспечения доступа к информации о деятельности государственных органов и органов местного самоуправления, в том числе к информации о деятельности судов в Российской Федерации.

3. Законодательство об информационной безопасности. Взаимная передача сведений, составляющих государственную тайну, органами государственной власти, предприятиями, учреждениями и организациями (ст. 16 Закона РФ «О государственной тайне»).

Объектом данного правонарушения являются охраняемые законом сведения, которые составляют государственную тайну и представляют большую ценность для государства и общества.

Объективная сторона этого правонарушения заключается в нарушении правил взаимной передачи сведений, составляющих государственную тайну, между органами государственной власти, предприятиями, учреждениями и организациями, не состоящими в отношении подчиненности и не выполняющими совместные работы. Эта передача осуществляется без санкции органа государственной власти, в распоряжении которого находится закрытая информация.

Субъективная сторона правонарушения может характеризоваться виной в виде умысла или неосторожности.

Субъекты правонарушения — руководители указанных органов, предприятий, учреждений и организаций, которые несут персональную ответственность за совершение данного правонарушения в рамках законодательства (санкция не расшифрована) должностные лица и граждане, виновные в нарушении законодательства Российской Федерации о государственной тайне, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.

4. Некоторые составы преступлений в сфере высоких технологий, определяемые гл. 28 УК РФ.

Первый состав — неправомерный доступ к компьютерной информации (ст. 272 УК РФ) — характеризуется следующим образом: объективная сторона преступления заключается в незаконном доступе к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в ЭВМ, в системе ЭВМ или их сети неправомерном доступе к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации; субъективная сторона определяется виной в форме умысла; субъект — лицо, достигшее 16 лет.

Второй состав — создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) — характеризуется так: объективная сторона состоит в незаконном создании программ для ЭВМ и внесении изменений в существующие программы, которые приводят к уничтожению, блокированию и иным негативным последствиям в деятельности ЭВМ и их сетей, а также использование и распространение подобных программ создании, распространении или использовании компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации; субъективная сторона преступления — вина в форме прямого умысла; субъект преступления — лицо, достигшее 16-летнего возраста.

Третий состав — нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) — имеет следующие характеристики: объективная сторона выражается в нарушении регламентированных правил эксплуатации средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, если это повлекло за собой существенный вред уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб; субъективная сторона данного незаконного проявления характеризуется виной в форме умысла и неосторожности; субъект здесь — лицо, имеющее доступ к рассматриваемым техническим средствам.

Необходимо подчеркнуть, что у всех трех исследуемых правонарушений в сфере компьютерной информации один и тот же объект — общественно опасные деяния, посягающие на безопасность информации, определенные технические информационные системы и компьютерную технику.

Виды наказания за совершение данных преступлений в информационной сфере самые разные: штраф, исправительные работы, принудительные работы, ограничение свободы, лишение свободы.