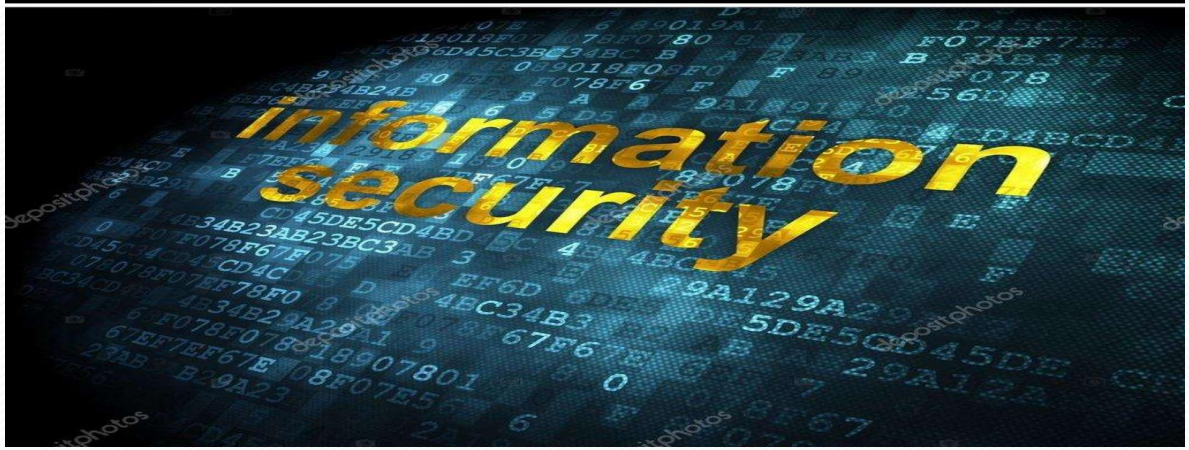

Основы
информационной
безопасности

- Исторические предпосылки направления ИБ
- Определение понятий информации, ИБ и основных составляющих ИБ (целостность, доступность, конфиденциальность)
- Общая характеристика информационной безопасности общества

- Задачи информационной безопасности общества
- Правовые основы информационной безопасности общества
- Угрозы безопасности ИБ

Информационная безопасность – совокупность мер по защите информационной среды общества и человека.



ГОСТ Р 50922-2006 Государственный стандарт Российской Федерации. Защита информации. Основные термины и определения

- **Защита информации** (ЗИ) - деятельность, направленная на предотвращение:
- **утечки защищаемой информации**,
- **несанкционированных и непреднамеренных воздействий** на защищаемую информации.

1) существует ли вообще в современной России государственная политика информационной безопасности

2) если существует, то при каких обстоятельствах, в какие периоды она формировалась и каким образом реализуется.

Становление защиты информации в России

Период	Факторы влияния	Деятельность по защите	Органы защиты
XVII в.	Образование российского централизованного государства, формирование органов государственного управления, развитие международных связей	Использование дезинформации; введение ограничений на въезд; шифрование переписки; введение ответственности за разглашение информации. Ответственность за шпионаж и государственную измену. Ответственность за хищение и подделку документов и печатей. Вопросы защиты информации в Судебниках 1497 и 1550 гг.	Оружейный, Казённый, Посольский приказы. Приказ тайных дел
XVIII в.	Развитие торгово-промышленной деятельности, появление акционерных компаний, кредитные отношения, биржевая деятельность	Расширение состава защищаемой информации	Преображенский Приказ, Верховный тайный совет. Военная Коллегия. Коллегия иностранных дел. Тайная розыскных дел Канцелярия. Тайная экспедиция
XIX в.	Новые формы акционерных обществ, промышленная революция	Ограничение на публикацию сведений, полученных по служебным каналам. Защита коммерческой тайны (тайны торговых, купеческих книг). Законодательство в области патентного и авторского права. Цензурные уставы	Государственный Совет. 1-й и 3-й отдел Собственной Его императорского величества канцелярии. Главное управление по делам печати. Особый отдел Департамента полиции. Технический комитет
Начало XX в.	Первая мировая война	Закон «О государственной измене путём шпионажа». Создание «закрытых» зон. Расширение состава защищаемой информации. Военно-промышленная тайна. Защита информации в процессе радиотелеграфных переговоров	Министерство внутренних дел, Департамент полиции, Военное министерство, Комитет для защиты промышленной собственности

Защита информации в СССР (1917–1995)

Период	Факторы влияния	Деятельность по защите	Органы защиты
1917–1945	Изменение политического и экономического строя	Отмена коммерческой тайны. Увеличение объёма сведений, составляющих гостайну. Активизация иностранных спецслужб по добыванию информации о политическом, экономическом и военном положении СССР. Централизация управления защитой госсекретов. Усиление ответственности за разглашение гостайны, утрату секретных документов и халатное обращение с ними	Спец. органы защиты информации (спец. отдел ВЧК-ГПУ, далее — 7-й отдел НКВД)
1945-1975	Холодная война	Введение должности заместителя начальника объекта по режиму. Расширение объёма и тематики защищаемой информации и категорирование её по степени секретности. Ужесточение режима секретности. «Перечень сведений, составляющих гостайну» (1948). «Инструкция по обеспечению сохранения гостайны в учреждениях и на предприятиях СССР» (1948	Министерство государственной безопасности (1946). Комитет государственной безопасности при Совете министров СССР (1954)
1975-1995	Появление информационных войн и противоборства	Появление новых носителей информации, автоматизированных систем и распределенных систем обработки данных. Широкомасштабное применение средств технической разведки.	Государственная техническая комиссия по противодействию иностранным техническим разведкам (1973)

ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ ИБ КАК НАУКИ

- Формализация положений теории информационной безопасности
- Безопасность критически важных объектов
- Разработка средств и методов противодействия угрозам информационной войны (в частности разработка кибероружия (программное обеспечение или оборудование, предназначенные для нанесения ущерба в киберпространстве) (DDoS-атак, Компьютерные черви Stuxnet, шпионаж на информ. пространстве, кража данных…);
- Применение облачных технологий (безопасное хранение данных не на сервере, а в облаке)
- Защита личных данных
- Вопросы обеспечения безопасности в глобальных информационных сетях, например Internet
- Безопасность мобильных устройств
- Обеспечение достоверности информации в глобальных информационных системах,
- Расширение криптографии (применение блокчейн технологий. Блокчейн стал бесценным инструментом, идеально подходящим для обеспечения безопасности, но он также используется для таких задач, как хранение и подтверждение данных – метод, который в настоящее время используется для интеллектуального анализа данных (дата-майнинг). Блокчейн – это результат многолетних достижений в криптографии и информационной безопасности.
- Большие данные (Big Data)
- Более широкое использование многофакторной аутентификации
- Продолжающееся развитие искусственного интеллекта (ИИ)
- Подготовка кадров в области ИБ

Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 08.06.2020) «Об информации, информационных технологиях и о защите информации»:

ИНФОРМАЦИЯ - сведения (сообщения, данные) независимо от формы их представления.

Информационная безопасность Российской Федерации (далее - информационная безопасность) - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

Понятие информационной безопасности

- **Конфиденциальность**
- **Целостность**
- **Доступность**

ЖИЗНЕННО ВАЖНЫЕ ИНТЕРЕСЫ ОБЩЕСТВА В ИНФОРМАЦИОННОЙ СФЕРЕ

1. Обеспечение интересов общества.
2. Построение правового государства.
3. Построение информационного общества.
4. Сохранение нравственных ценностей общества.
5. Предотвращение манипулирования массовым сознанием.
6. Приоритетное развитие современных информационных технологий.

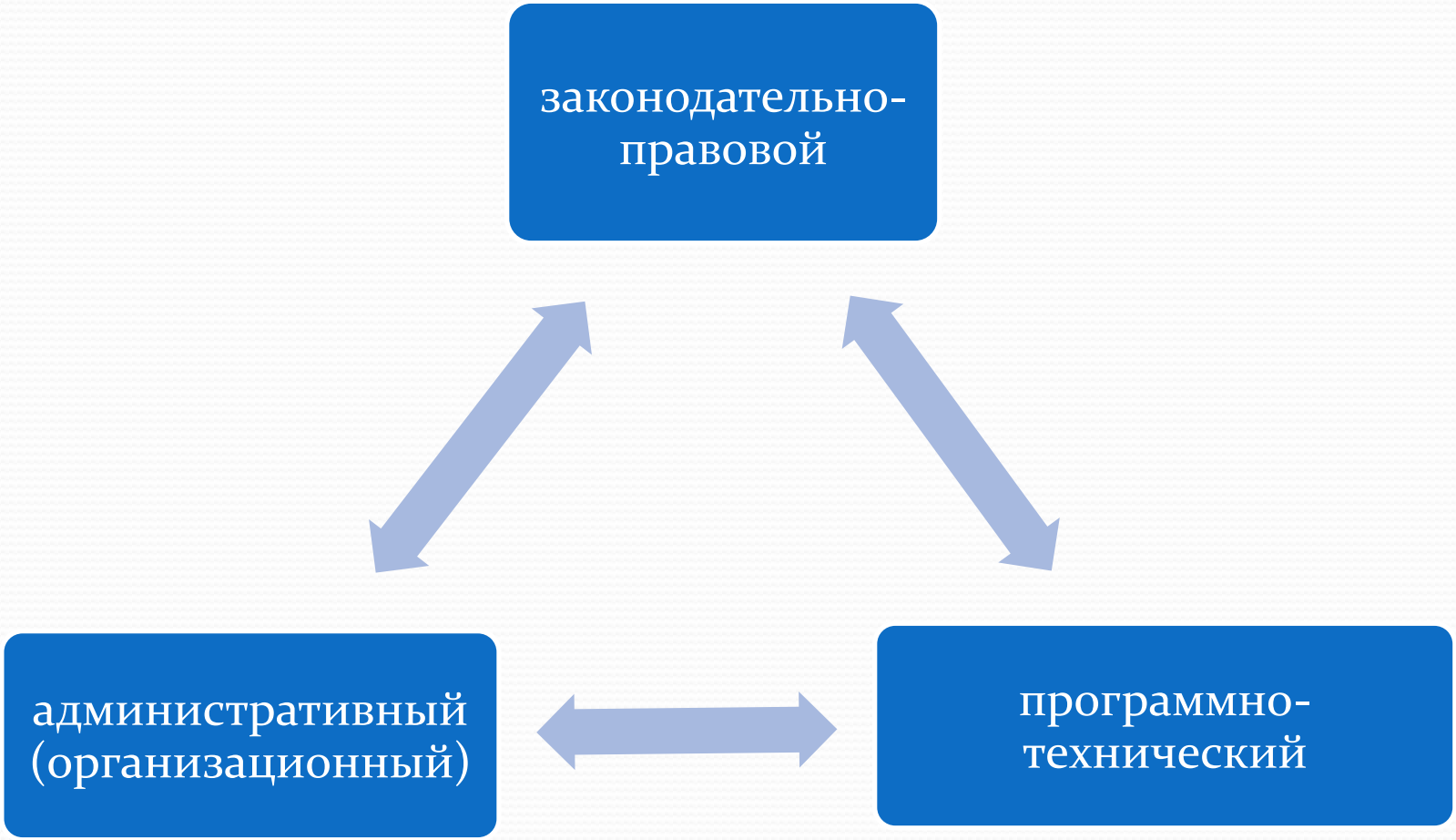
Основные средства информационно-психологического воздействия на человека

- **средства массовой коммуникации** (в том числе информационные системы, например, интернет и т.п.);
- **литература** (в том числе, художественная, научно-техническая, общественно-политическая, специальная и т.п.);
- **искусство** (в том числе, различные направления так называемой массовой культуры и т.п.);
- **образование** (в том числе, системы дошкольного, среднего, высшего и среднего специального государственного и негосударственного образования, система так называемого альтернативного образования и т.п.);
- **воспитание** (все разнообразные формы воспитания в системе образования, общественных организаций - формальных и неформальных, система организации социальной работы и т.п.);
- **личное общение**.

Задачи информационной безопасности

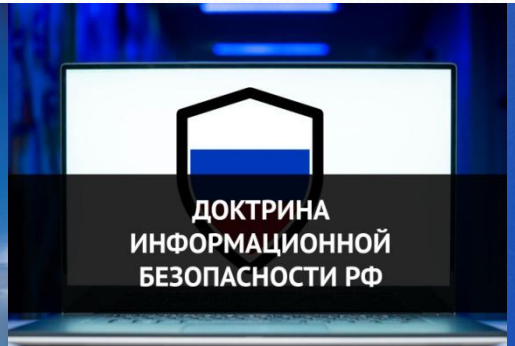
- защита *государственной тайны*, т. е. информации, являющейся собственностью государства;
- защита прав граждан на владение, распоряжение и управление принадлежащей им информацией, т.е. *персональные данные*;
- защита прав предпринимателей при осуществлении ими коммерческой деятельности, т.е. *коммерческая тайна*;
- защита конституционных прав граждан на тайну переписки, переговоров, личную тайну.

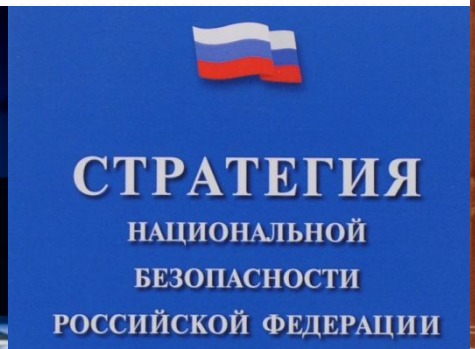
УРОВНИ ФОРМИРОВАНИЯ РЕЖИМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

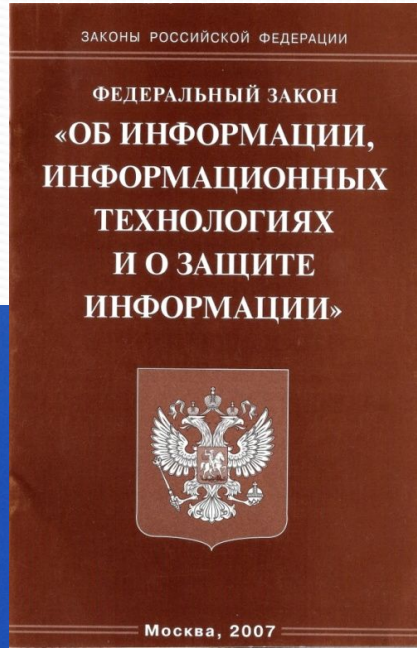


Конфиденциальная информация

- 1. Персональные данные
- 2. Тайна следствия и судопроизводства
- 3. Служебная тайна
- 4. Профессиональная тайна
- 5. Коммерческая тайна
- 6. Тайна о сущности изобретения, полезной модели или пром.образца до официальной публикации информации о них







Нормативно-правовые акты в области защиты персональных данных

- Концепция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.)
- Директива Европейского Союза **№2002/58/ЕС** "О приватности и электронных коммуникациях"
- Трудовой кодекс Российской Федерации **от 30.12.2001 г.№ 197-ФЗ** - Глава 14 «Защита персональных данных работника»
- Федеральный закон **от 19.12.2005 г. №160-ФЗ** «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»
- Федеральный закон **от 27.07.2006 г. № 149 –ФЗ** «Об информации, информационных технологиях и о защите информации»
- Федеральный закон **от 27.07.2006 г.№ 152-ФЗ** «О персональных данных»
- Федеральный закон Российской Федерации **от 25.07.2011 г.№ 261-ФЗ** "О внесении изменений в Федеральный закон "О персональных данных"
- Федеральный закон **от 30.12.2015 г.№ 439-ФЗ** "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях"
- Федеральный закон **от 21.07.2014 г.№242-ФЗ** "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях"
- Указ Президента Российской Федерации **от 06.03.1997 г.№188** «Об утверждении перечня сведений конфиденциального характера»
- Указ Президента Российской Федерации **от 30.05.2005 г.№ 609** «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»
- Указ Президента Российской Федерации **от 17.03.2008 г. №351** «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
- Распоряжение Президента Российской Федерации **от 10.07.2001 г. № 366-РП**«О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных»
- Постановление Правительства Российской Федерации **от 21.03.2012 г. № 211** «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»
- Постановление Правительства Российской Федерации от **03.11.1994 г. № 1233** «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использования атомной энергии и уполномоченном органе по космической деятельности»
- Постановление Правительства Российской Федерации **от 01.11.2012 г. №1119** «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Постановление Правительства Российской Федерации **от 06.07.2008 г. № 512 «**Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»
- Постановление Правительства Российской Федерации от **15.09.2008 г.№ 687«Об** утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
- Постановление Правительства РФ от 04.03.2010 г**.№ 125** "О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию"
- Приказ Роскомнадзора от 05.09.2013 г**.№ 996** «Об утверждении требований и методов по обезличиванию персональных данных»
- Распоряжение Правительства Российской Федерации **от 15.08.2007 г. №1055-Р** «О плане подготовки проектов нормативных актов, необходимых для реализации Федерального закона «О персональных данных»
- Приказ ФСБ России от **09.02.2005 г.№ 66** «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации. Положение ПКЗ 2005)»
- Приказ ФСТЭК России **от 18.02.2013 г.№ 21** «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- Приказ Минкомвязи России **от 20.07.2017 г.№ 373** "О признании утратившими силу приказов Министерства связи и массовых коммуникаций РФ" от 21 декабря 2011 №346, от 28 августа 2015 №315 и п.9 приказа Министерства связи и массовых коммуникаций РФ от 24 ноября 2014 №403
- Приказ Роскомнадзора **от 30.05.2017 г.№ 94"**Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения"

Контроль
за выполнением законодательства в области защиты ПДн
возложен на следующие органы:

- Уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) – основной надзорный орган в области персональных данных;
- ФСБ – основной надзорный орган в части использования средств шифрования;
- ФСТЭК – надзорный орган в части использования технических средств защиты информации.

Законодательство в области защиты сведений, составляющих тайну следствия и судопроизводства

- Уголовного процессуального кодекса Российской Федерации [ст. 161)
- Федеральным законом от 20 августа 2004 года N 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» (ст. 9)

Законодательство в области защиты служебной тайны

- ФЗ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»
- Указ президента России от 06.03.97 года № 188 «Об утверждении перечня сведений конфиденциального характера»(**23 сентября** 2005 г., 13 июля 2015 г.)
- Постановление Правительства РФ от 03.11.1994 N 1233 (ред. от 06.08.2020) "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности«
- Ст. 3.1 «Служебная тайна в области обороны» ФЗ от 31 мая 1996 г. № 61-ФЗ (с изм. от 11.06.2021 г.) «Об обороне»

Законодательство в области защиты профессиональной тайны (некоторые НПА в качестве примеров)

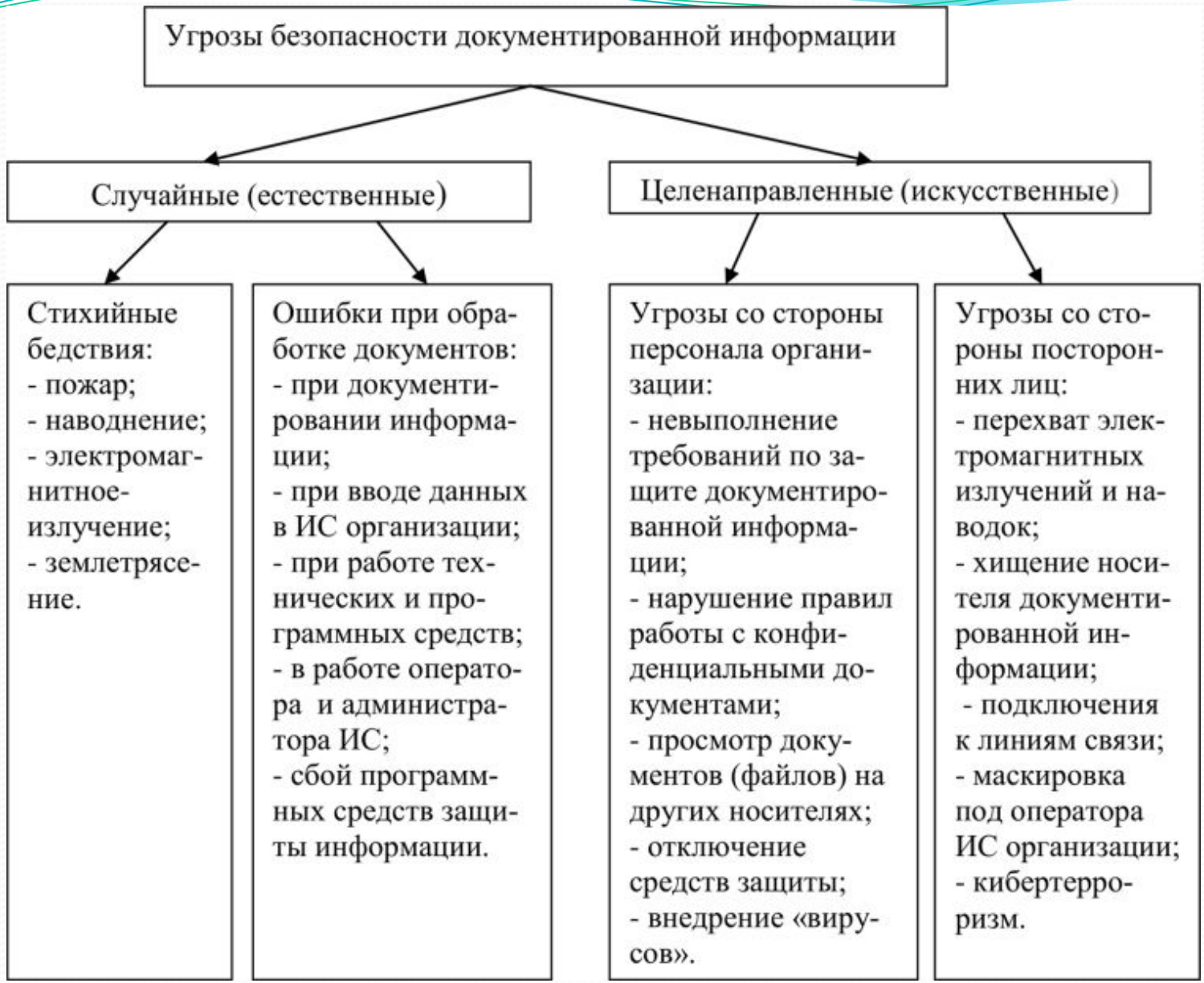
- **Врачебная тайна**:
  - ✔ Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ;
  - ✔ Статья 13. «Соблюдение врачебной тайны» Федеральный закон от 21.11.2011 N 323-ФЗ (ред. от 02.07.2021) "Об основах охраны здоровья граждан в Российской Федерации" (с изм. и доп., вступ. в силу с 01.10.2021)
- **Тайна связи**: Федеральный закон "О почтовой связи" от 17.07.1999 N 176-ФЗ ;Уголовным кодексом Российской Федерации (ст. 138)
- **Нотариальная тайна**: ст.5 "Основ законодательства Российской Федерации о нотариате" (утв. ВС РФ 11.02.1993 N 4462-1) (ред. от 27.12.2019) (с изм. и доп., вступ. в силу с 11.05.2020)
- **Банковская тайна:** Федеральный закон "О банках и банковской деятельности" от 02.12.1990 N 395-1

Коммерческая тайна

- ФЗ от 29.07.2004 № 98-ФЗ «О коммерческой тайне»
- ФЗ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»

Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

- Часть 4 ГК РФ
- Указ Президента РФ 06.03.1997 № 188 "Об утверждении Перечня сведений конфиденциального характера«
- ФЗ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» - действия Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, за исключением случаев, предусмотренных статьей 15.2 настоящего ФЗ .


Угрозы безопасности документированной информации
Случайные (естественные)
Целенаправленные (искусственные)
Стихийные бедствия:
- пожар;
- наводнение;
- электромагнитное-излучение;
- землетрясение.
Ошибки при обработке документов:
- при документировании информации;
- при вводе данных в ИС организации;
- при работе технических и программных средств;
- в работе оператора и администратора ИС;
- сбой программных средств защиты информации.
Угрозы со стороны персонала организации:
- невыполнение требований по защите документированной информации;
- нарушение правил работы с конфиденциальными документами;
- просмотр документов (файлов) на других носителях;
- отключение средств защиты;
- внедрение «вирусов».
Угрозы со стороны посторонних лиц:
- перехват электромагнитных излучений и наводок;
- хищение носителя документированной информации;
- подключения к линиям связи;
- маскировка под оператора ИС организации;
- кибертерроризм.

ТИПЫ УГРОЗ

Относящиеся к личной безопасности:

- Ознакомление с порнографическими материалами, ненормативной лексикой, информацией суицидального характера, расистского, человеконенавистнического или сектантского содержания.
- Угроза получения недостоверной или ложной информации.
- Формирования зависимости (игровой, компьютерной, от интернета).
- Общение с опасными людьми (извращенцы, мошенники).
- Привлечение к выполнению противоправных действий (хакерство, нарушение прав и свобод других).

Касающиеся общей безопасности:

- Материалы, существование и использование которых может стать причиной посягательства на безопасность окружающих (например, информация о создании оружия или ядовитых веществ).
- Сознательное и бессознательное введения в заблуждение других.
- Совершение противоправных действий, влекущих за собой ответственность согласно действующему законодательству.
- Кибербуллинг — сознательная травля и унижение, прежде всего сверстников.

Связанные с утечкой персональной информации (в т.ч. Фишинговые атаки):

- Разглашение личной и конфиденциальной информации (фамилии, имена, контакты, данные кредитных карт, номера телефонов).
- Угроза заражения ПК вирусами различной категории.
- Опасность загрузки программ с вредными функциями.

Памятка. Основные правила безопасной работы в Интернете

- Не давайте никому свои пароли.
- Не передавайте никому личную информацию без крайней на то необходимости.
- Не реагируйте на неприличные и грубые комментарии, адресованные вам.
- Отказывайтесь от встреч со случайными людьми, с которыми познакомились в Интернете. Не делитесь своими фото с незнакомцами.
- Не сообщайте информацию о банковских картах (номер карты, срок действия и тайный код).
- Не скачивайте и не устанавливайте неизвестные программы по ссылкам, даже если их предоставили друзья.
- Устанавливая проверенные программы, контролируйте, чтобы на ПК не добавились нежелательные программы.
- Не смотрите информацию по неизвестным ссылкам (друзья, которые ими делятся, могут не подозревать об угрозе).
- Не открывайте письма со спамом, они могут содержать вирусы.

Помните:

- Когда вы разместили информацию в Интернете, вы теряете над ней контроль. Удаление материала и его копий практически невозможно.
- Вы должны точно знать, кому предоставляете информацию, а также, как и с какой целью она будет использована.
- Думайте: Стоит ли размещать информацию, если вы не знаете, как ее используют и не навредит ли это вам или близким?

Тематика докладов по дисциплине «Безопасность жизнедеятельности»
Раздел «Информационная безопасность»

1. Информация - фактор существования и развития общества. Основные формы проявления информации, её свойства как объекта безопасности.
2. Соотношение понятий «информационная безопасность» и «национальная безопасность»
3. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.
4. Информационное оружие и его классификация.
5. Управление и защита информации в информационно-телекоммуникационных сетях.
6. Кибербезопасность: как защитить личные данные в сети
7. Безопасность в сети Интернет
8. Угрозы безопасности в сети интернет (целостности, дотупности, конфиденциальности, кибербуллинг, груминг, секстинг и т.д.)
9. Фишинг , как угроза безопасной работе в сети Интернет. Способы проявления фишинговых атак.
10. Социальная инженерия в контексте информационной безопасности.
11. Кибервойны как современная реалия.
12. Кибервойска России и зарубежных стран. Их цели и задачи.
13. Информационно-психологическое воздействие
14. Законодательные основы безопасности детей в сети Интернет
15. Социальные сети как источник угроз безопасности личной информации
16. Безопасность мобильных приложений.
17. Нарушение закона «О персональных данных» на примере работы Мобильного приложения GetContact .
18. Основы цифровой гигиены