

**«Основы информационной  
безопасности.  
Нормативно-правовое обеспечение  
информационной безопасности»**

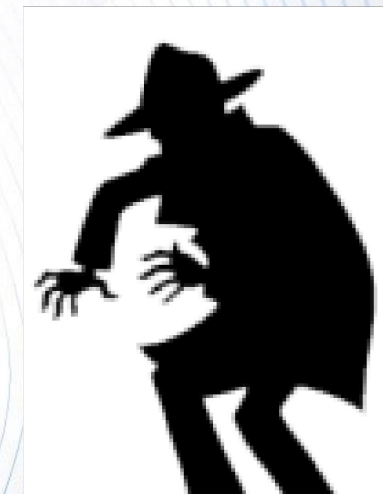


## Абзалов Олег Накибович

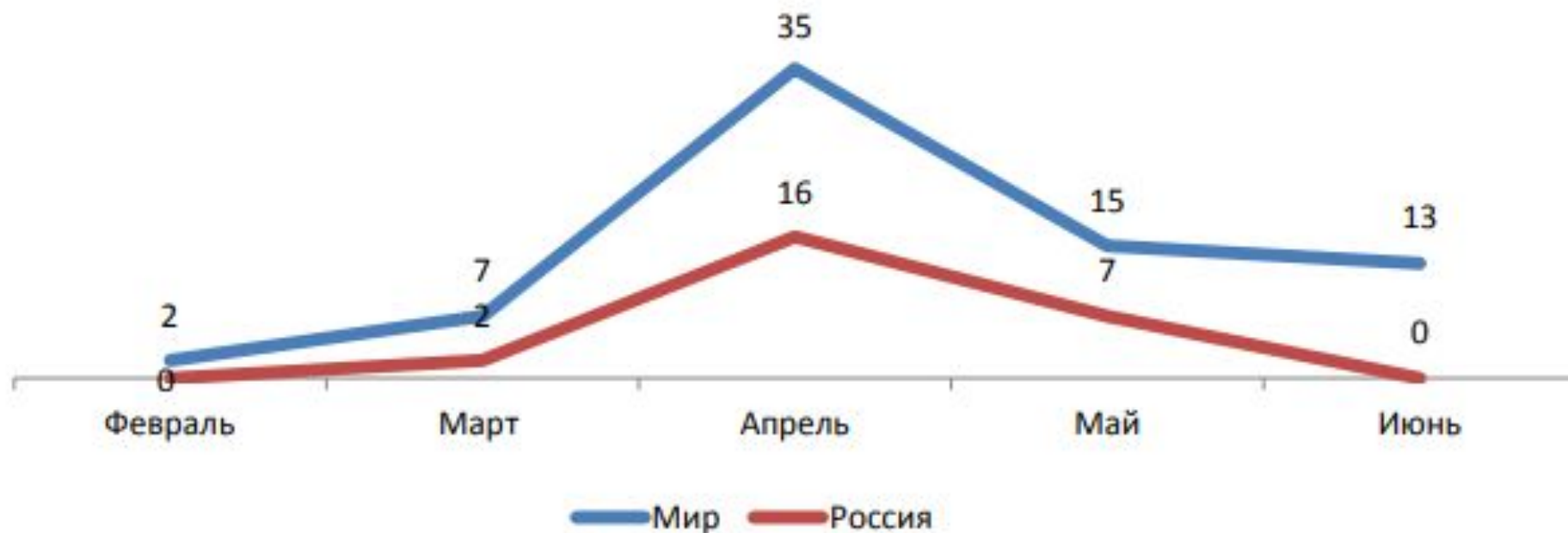
- преподаватель и эксперт-практик в области информационной безопасности и комплексной защиты информации;
- автор учебных программ и курсов в вузах Москвы по дисциплинам “Информационная безопасность”, “Аудит информационной безопасности”, “Защита информации ограниченного доступа”, “ИТ-безопасность”;
- доступ к ГТ (ф. 2);
- стаж работы руководителем проектов в разработке систем защиты персональных данных более 16 лет;
- консультант по вопросам информационной безопасности международной ассоциации «Генералы Мира за Мир».

# Актуальность проблемы обеспечения безопасности персональных данных

«Кто владеет информацией – тот владеет миром...»  
сэр У. Черчилль

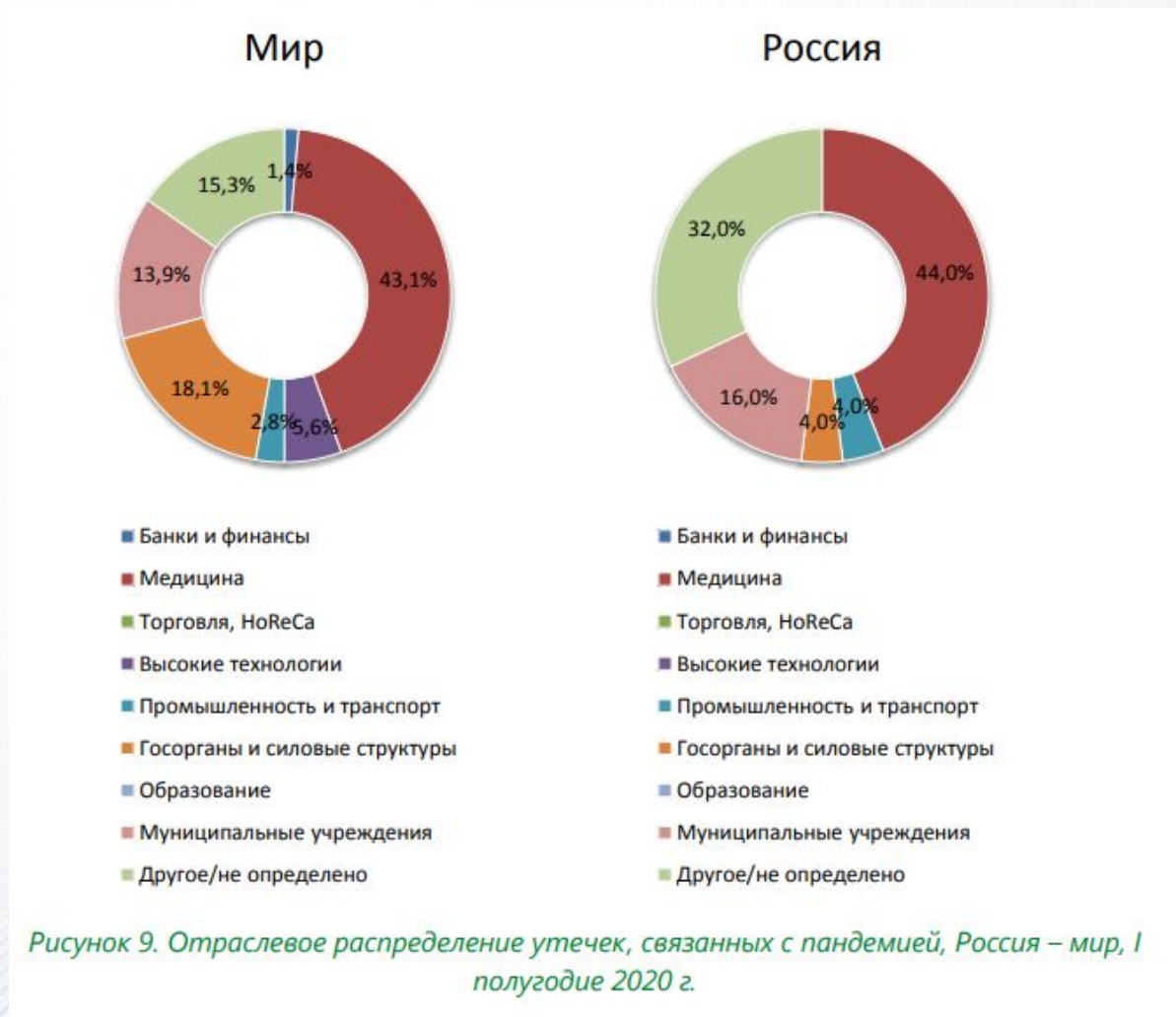


## Статистика зафиксированных утечек информации

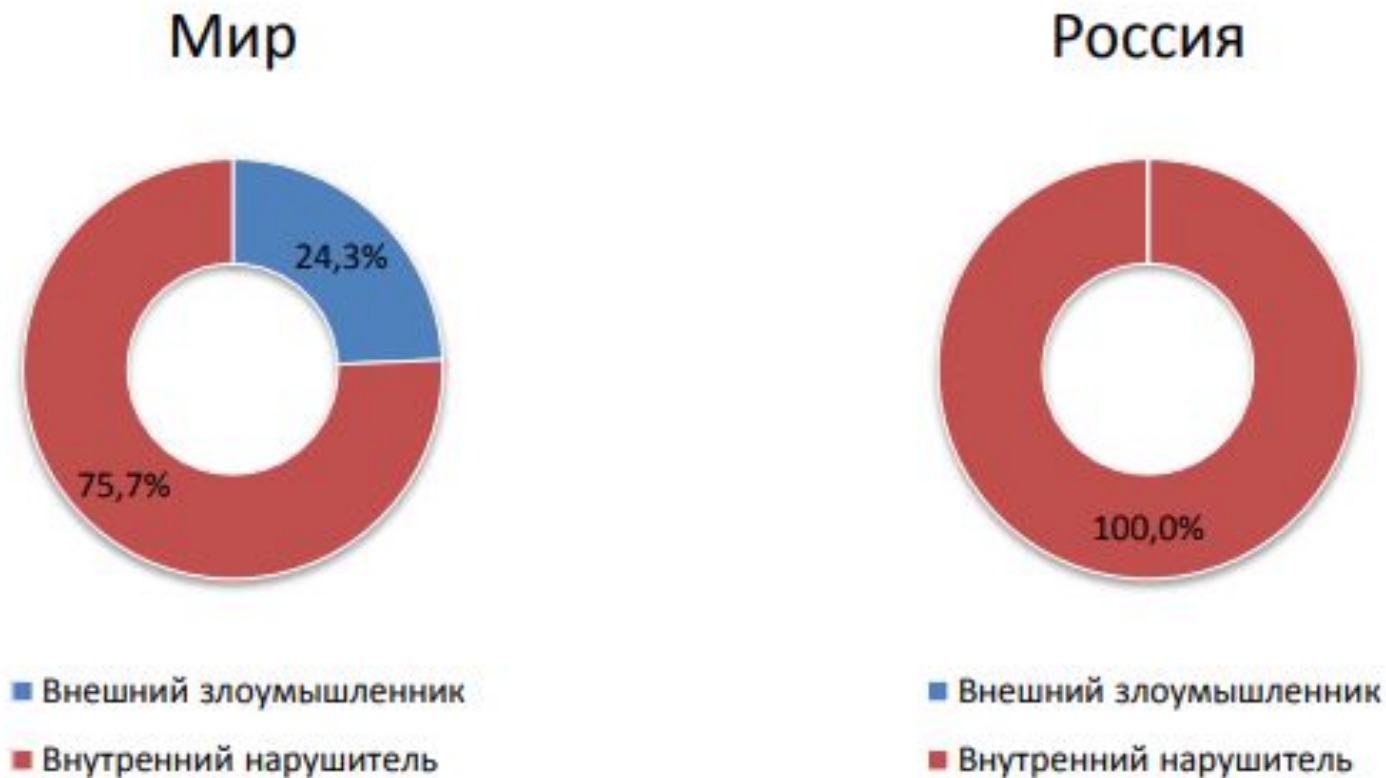


*Рисунок 1. Число зафиксированных утечек, связанных с пандемией. Россия – мир, I полугодие 2020 г.*

# Каналы утечек по отраслевой принадлежности



## Каналы утечек по источникам угроз



*Рисунок 5. Распределение утечек, связанных с пандемией, по вектору воздействия, Россия – мир, I полугодие 2020 г.*

## Каналы утечек в мире

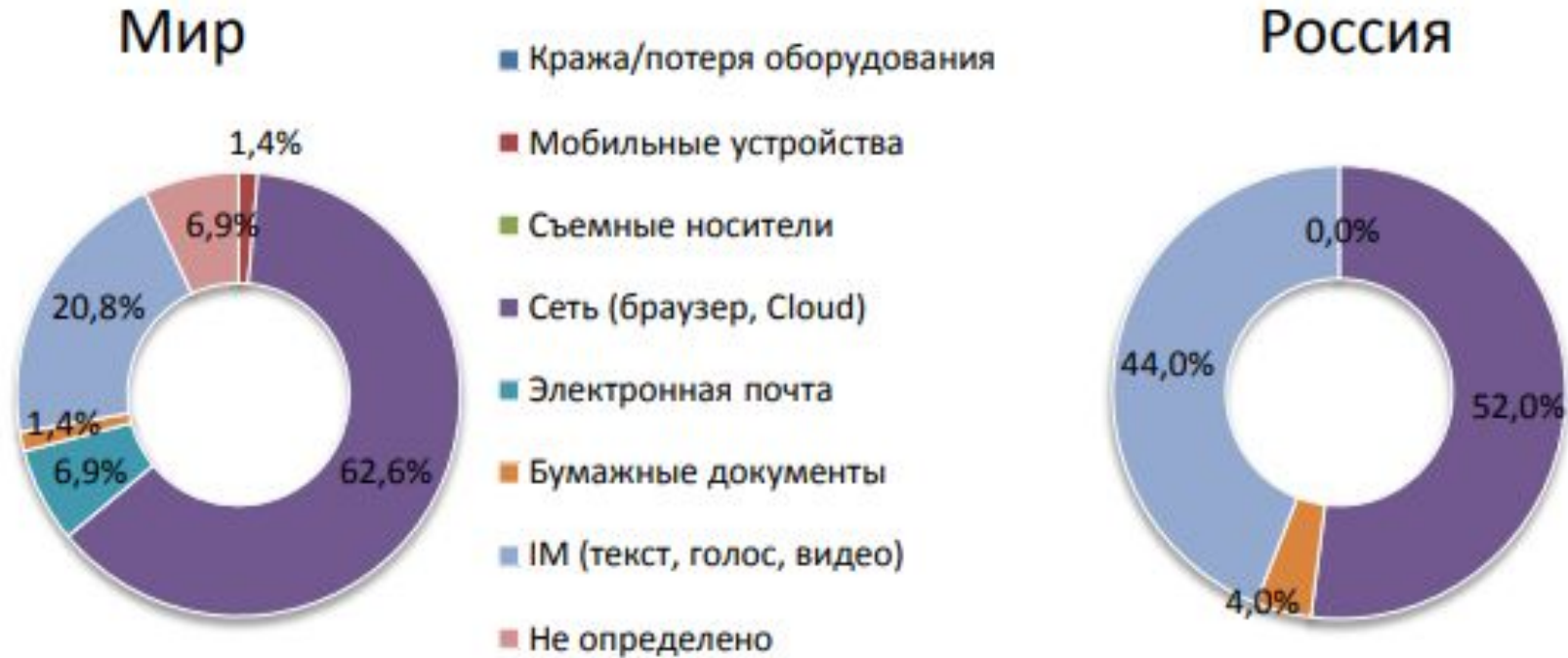


Рисунок 6. Распределение утечек, связанных с пандемией, по каналам, Россия – мир, I полугодие 2020 г.

## Реализованные утечки по странам

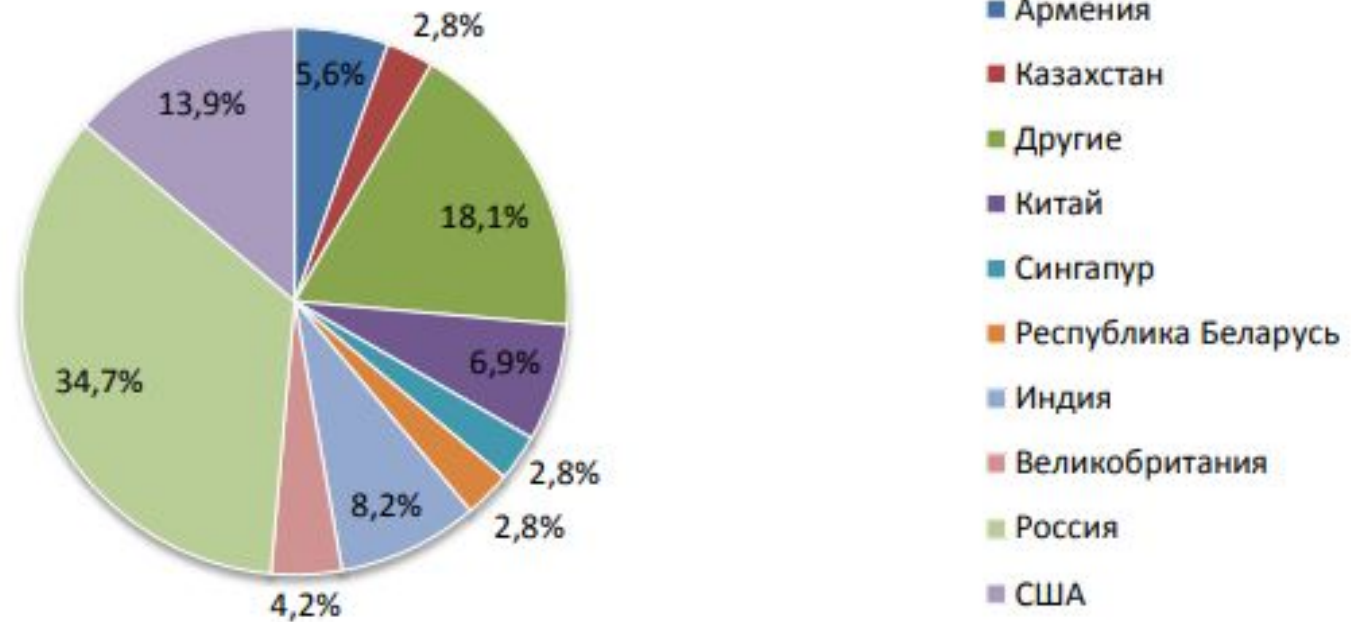


Рисунок 2. Распределение утечек, связанных с пандемией, по странам, I полугодие 2020 г.

Более трети зарегистрированных утечек произошли в России, на втором месте США, на третьем Индия



## Статистика распределения утечек

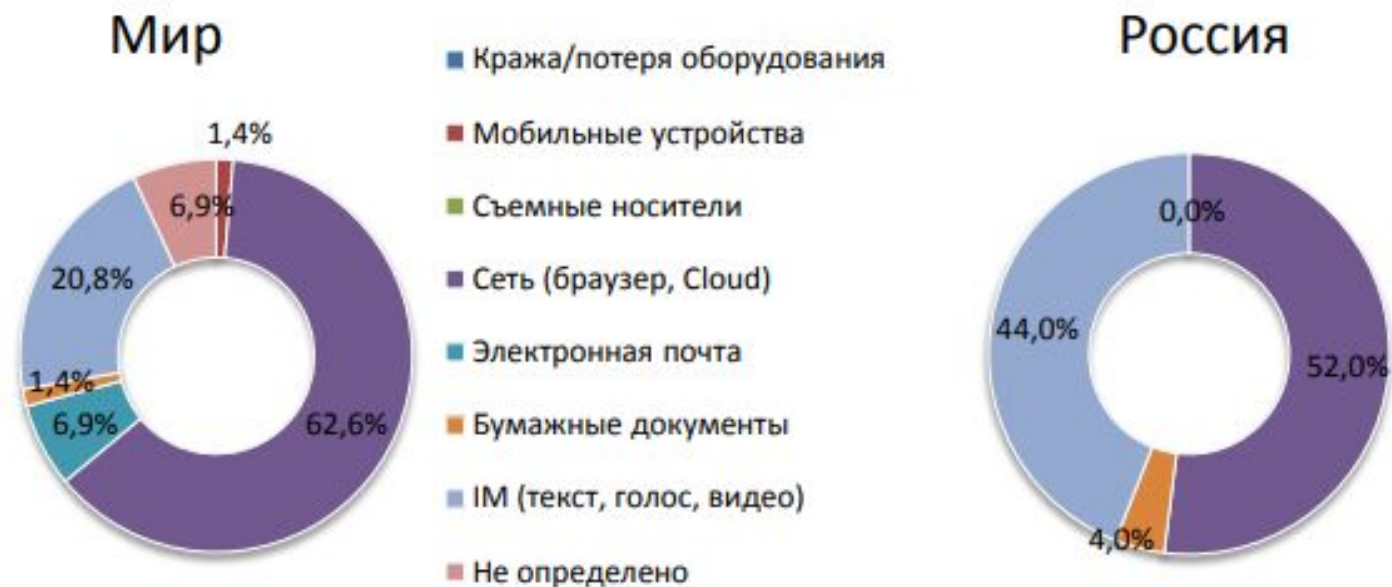


Рисунок 6. Распределение утечек, связанных с пандемией, по каналам, Россия – мир, I полугодие 2020 г.

**Свыше половины** случаев компрометации данных, связанных с пандемией, как в России,

так и в мире произошли **через сеть**

## Распределение утечек по типам данных



Рисунок 3. Распределение утечек, связанных с пандемией, по типам данных, Россия – мир, I полугодие 2020 г.

# Результаты исследования InfoWatch

**28 июня 2021.**

**Из облака утекли персональные данные пользователей**

**WordPress**

Группа исследователей **Website Planet** по главе с Йеремией Фаулером (Jeremiah Fowler) обнаружила не защищенную паролем базу данных **размером более 86 Гб.**

В облачном хранилище находились более 814 млн записей конфиденциальной информации, связанные с аккаунтами WordPress: **имена** пользователей и **адреса** электронной почты.

Также на сервере оказались раскрыты журналы с логами событий, утекла такая конфиденциальная информация, как **роли доступа** и **ID.**



## Основной источник нарушения ИБ

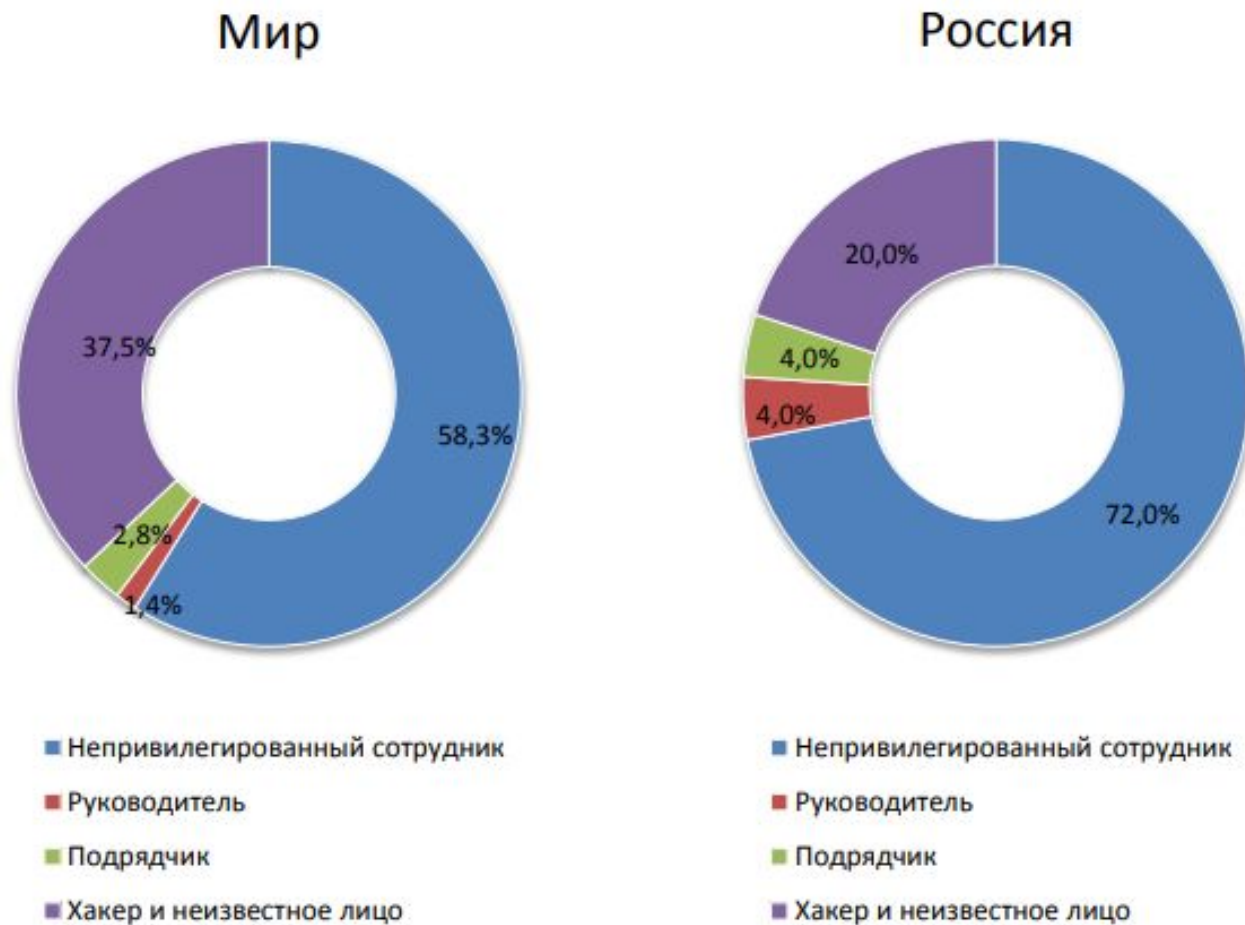


Рисунок 4. Распределение утечек по виновнику, Россия – мир, 2019 г.

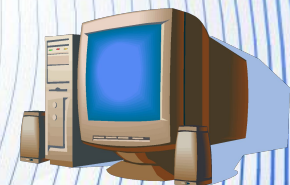
## Выводы

1. Динамика утечек, связанных с пандемией коронавируса, во многом **повторяет сценарий распространения** самой инфекции.
2. **Ближе к весне**, на пороге массовых заболеваний COVID-19 в мире, зарегистрированы **первые случаи компрометации данных**.
3. В марте-апреле, когда инфекция активно распространялась в европейских странах и США, происходил лавинообразный **рост числа утечек**.
4. Медицинским учреждениям и другим организациям, обрабатывающим данные людей с коронавирусом и связанную с ними информацию, удалось **усилить** направление информационной безопасности, **организационными мероприятиями**.
5. **Персонал** стал **более ответственно** относиться к защите конфиденциальных данных.
6. **Выросла информированность** широких масс о пандемии.
7. Люди **поняли**, что от заболевания новой инфекцией не застрахован никто, а утечка может принести **незаслуженные страдания**.
8. Пандемия коронавируса **высветила** ряд «болевых точек» в организации корпоративных систем ИБ.
9. **Подтвердился** невысокий уровень зрелости процессов управления ИБ в медицинской сфере, а также в ряде муниципальных и государственных структур (фактически, **независимо от страны**, где это происходило).

# Основные понятия в области технической защиты информации

**Информация** - сведения (сообщения, данные) независимо от формы их представления

- акустическая (речевая) информация
- видовая информация
- информация, обрабатываемая (циркулирующая) в ИС, в виде электрических, электромагнитных, оптических сигналов;
- информация, обрабатываемая в ИС, представленная в виде бит, байт, IP-протоколов, файлов и других логических структур.

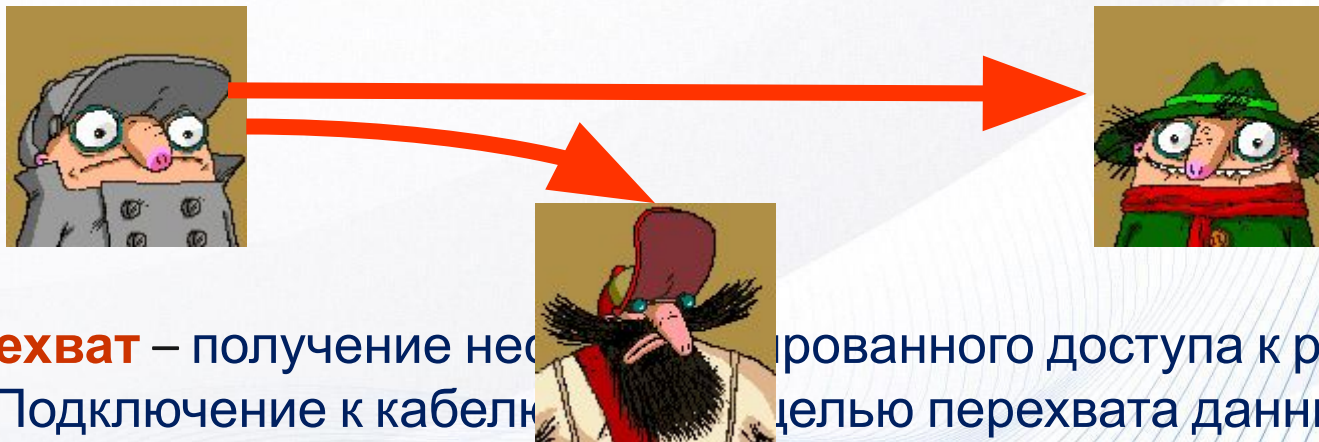
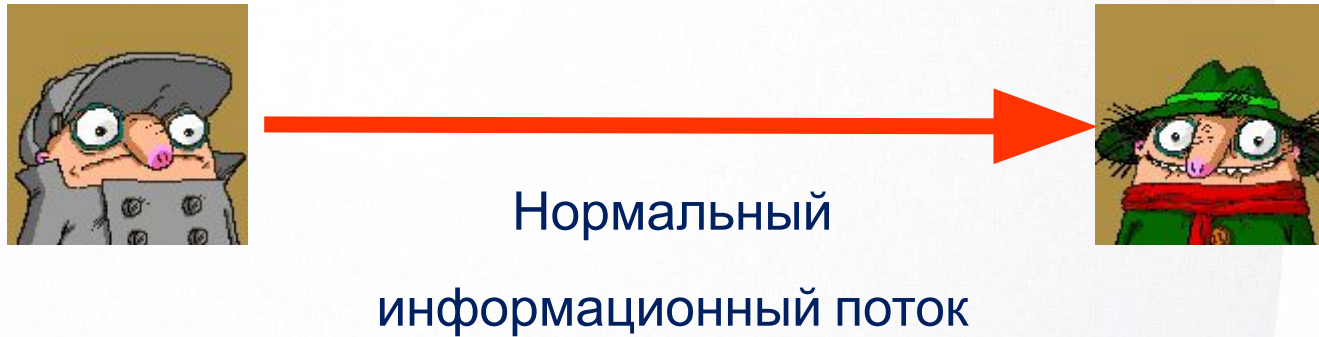


## Термины и определения

---

- **Конфиденциальность информации** – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.
- **Доступность информации** - состояние информации, характеризуемое способностью АС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.
- **Целостность информации** – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки и хранения.

## Нарушение конфиденциальности

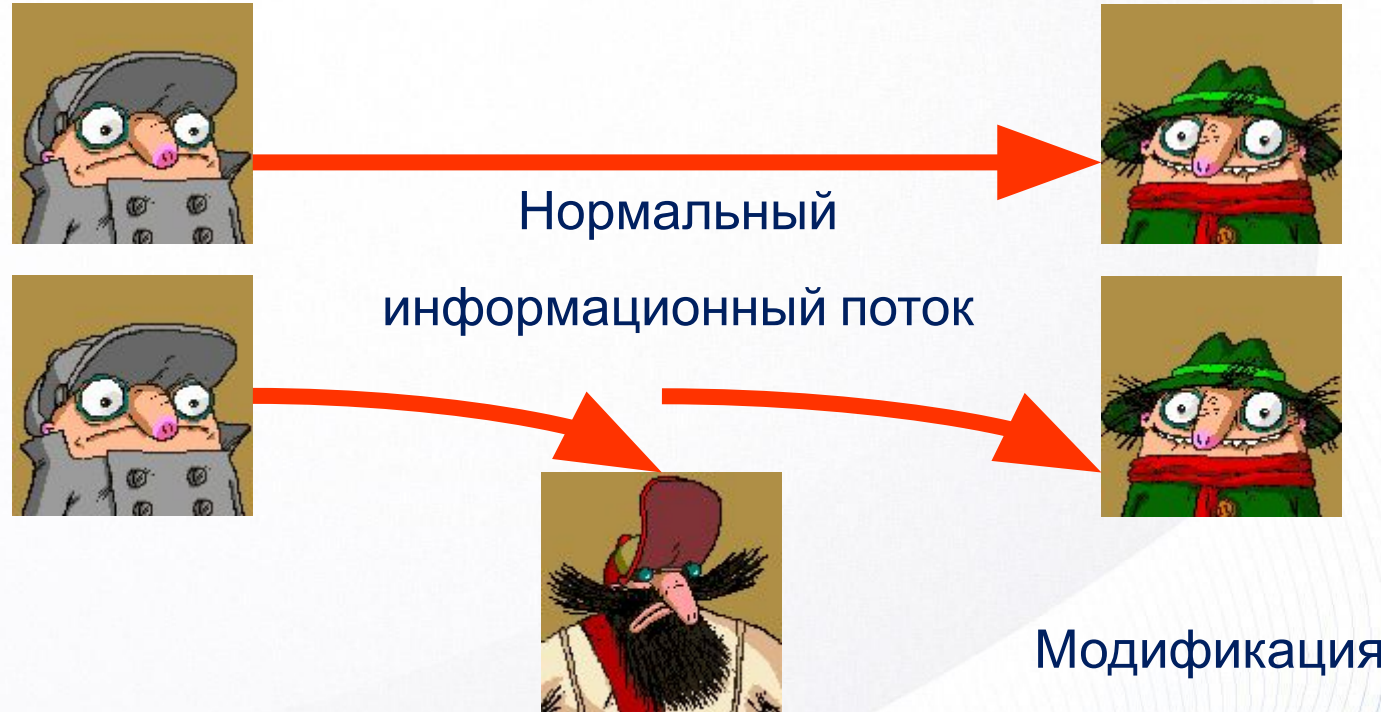


**Перехват** – получение несанкционированного доступа к ресурсу.

- Подключение к кабелю с целью перехвата данных
- Незаконное копирование файлов и программ



## Нарушение целостности



**Модификация** – открытие несанкционированного доступа к ресурсу и его изменение нарушителем.

- Изменение значений в файле данных
- Модификация кода программы с целью изменения ее функций
- Изменение содержимого передаваемого по сети сообщения

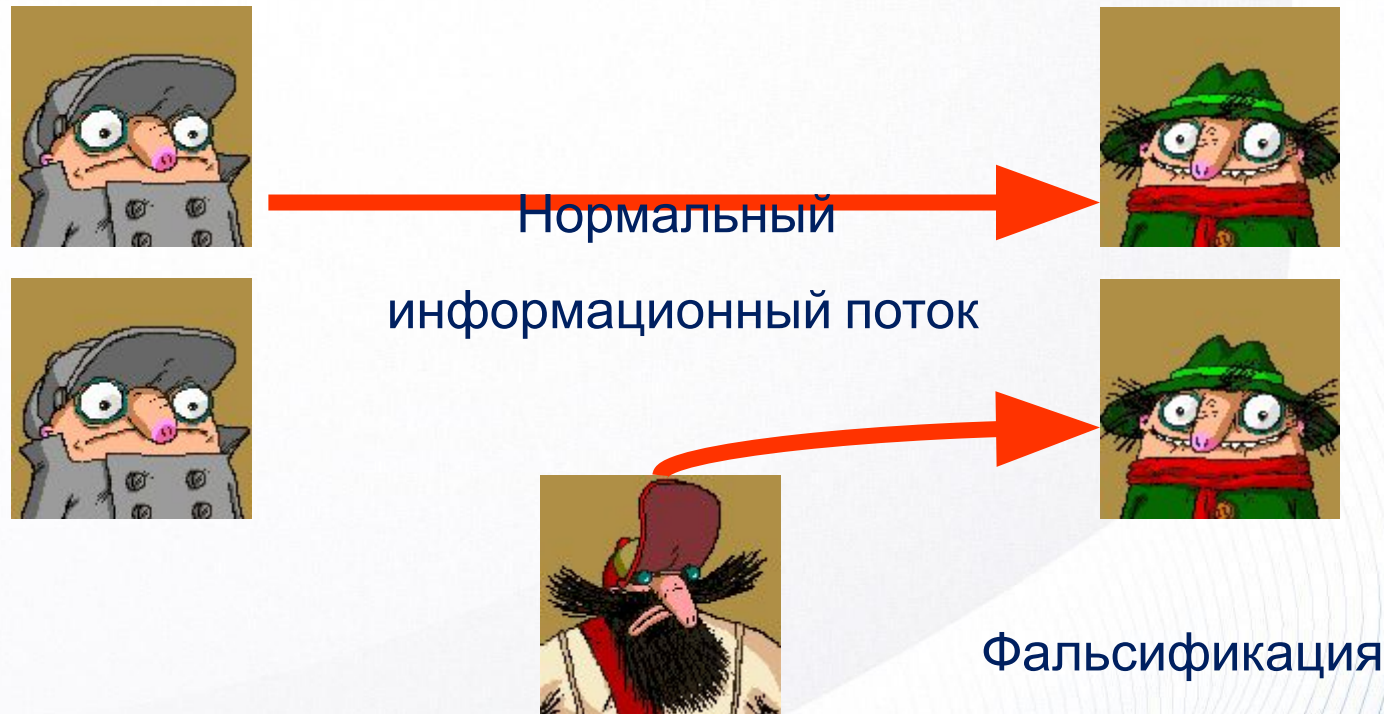
## Нарушение **доступности**



**Разъединение** – уничтожение ресурса системы, либо приведение его в состояние недоступности или негодности.

- Вывод из строя оборудования
- Обрыв линии связи
- Разрушение файловой системы

## Нарушение аутентичности



**Фальсификация** – внесение в систему ложного объекта.

- Отправка поддельных сообщений по сети
- Добавлений записей в файл

## Термины и определения

---

**Информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

**Информационно-телекоммуникационная сеть** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

## Термины и определения

---



**Обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

## Термины и определения

---

**Доступ к информации** - возможность получения информации и ее использования.

**Предоставление информации** - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

**Распространение информации** - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

## Термины и определения

---

**Электронное сообщение** - информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

**Документированная информация** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

**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.

## Термины и определения

---

**Информационная безопасность** - механизм защиты, обеспечивающий:

- **конфиденциальность**: доступ к информации только авторизованных пользователей;
- **целостность**: достоверность и полноту информации и методов ее обработки;
- **доступность**: доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости.





## Термины и определения

---

**Оператор информационной системы** – гражданин или юридическое лицо, осуществляющее деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

### **Оператор**

- государственный орган
- муниципальный орган
- юридическое лицо
- физическое лицо

совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с персональными данными.

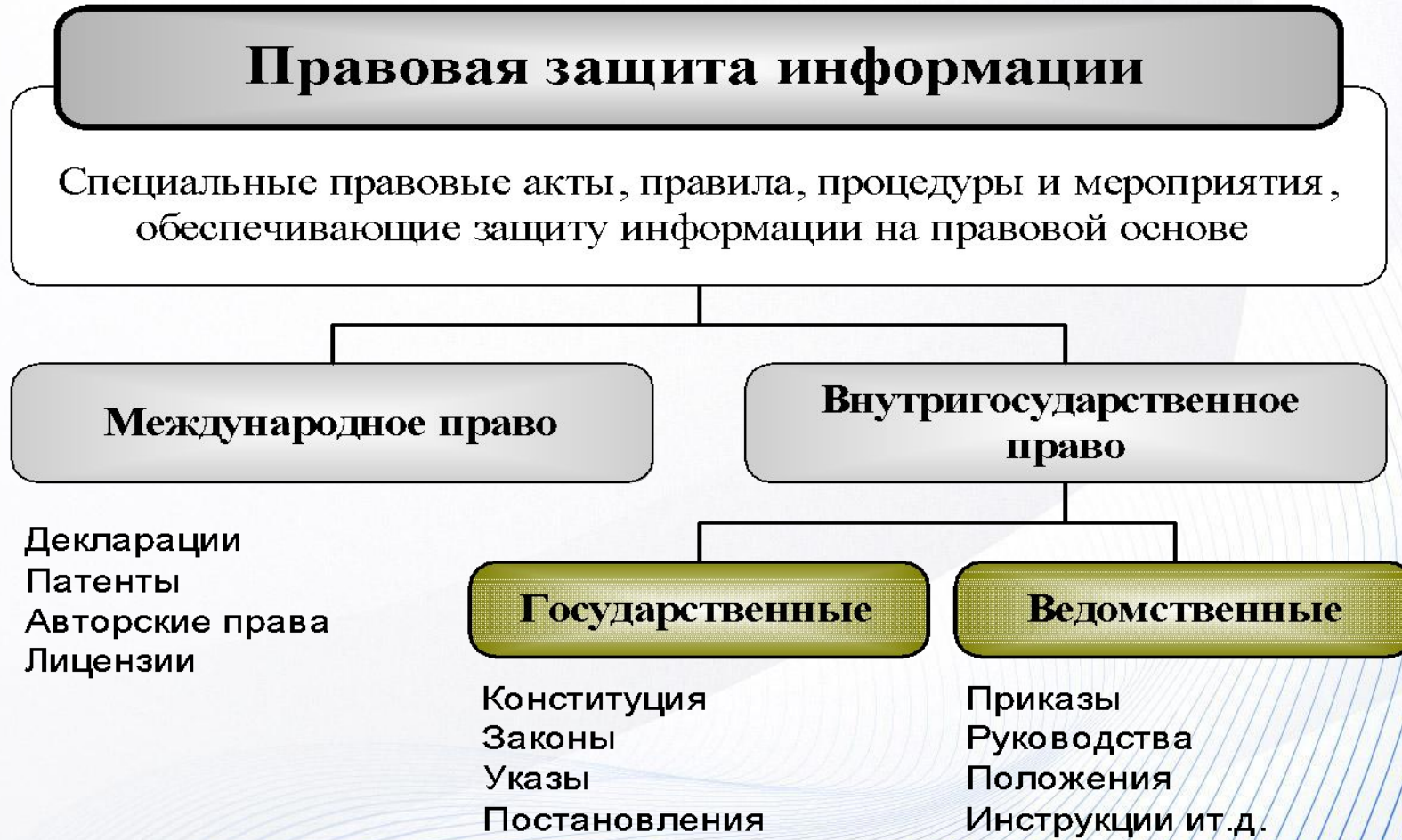
## Термины и определения

---

**Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными

- сбор
- запись
- систематизация
- накопление
- хранение
- уточнение (обновление, изменение)
- извлечение
- использование
- передача (распространение, предоставление, доступ)
- обезличивание

# Нормативные правовые акты и организационно-распорядительные документы по технической защите информации ограниченного доступа



# Конституция РФ

---

## **Статья 24.**

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

## **Статья 29.**

4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

## Положение о ГСЗИ в РФ от ИТР и от её утечки по техническим каналам

---

- **Определяет** задачи и структуру государственной системы защиты информации в Российской Федерации.
- **Является** документом, **обязательным для выполнения** при проведении работ по защите информации, содержащей сведения, составляющие **государственную или служебную тайну**, во всех органах власти и прочих организациях независимо от их организационно-правовой формы и формы собственности.

Постановление  
Правительства РФ  
№ 912-51 от 15 сентября 1993

# Организационная структура ГСЗИ



# Структура законодательства России по персональным данным



**Угрозы несанкционированного  
доступа к информации  
и  
реализации технического канала утечки  
информации**



## Угрозы НСД

### НСД

**(несанкционированные действия)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых ИС.



**Для реализации применяются**

программные средства

программно-аппаратные средства

## Угрозы утечки информации по техническим каналам

---

### **Описание угрозы утечки информации по ТКУИ:**

источник угрозы (приемник информативного сигнала)  
среда (путь) распространения информационного сигнала  
источник (носитель) информации

### **Источники угроз утечки информации по ТКУИ:**

физические лица, не имеющие доступа к ИС  
зарубежные спецслужбы или организации  
криминальные группировки



## ТКУИ, приводящие к возникновению угроз безопасности информации

**Технический канал утечки информации** - совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.



СТР-К



**Технический канал утечки информации** - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

# Угрозы утечки информации по техническим каналам

## Среда распространения информативного сигнала

Физическая среда, по которой информативный сигнал может распространяться и регистрироваться приемником.



# Последствия

## ТКУИ

**нарушение  
конфиденциальности**

**копирование,  
несанкционированное  
распространение**

## НСД

**нарушение  
конфиденциальности**

**копирование,  
несанкционированное  
распространение**

**нарушение  
целостности**

**уничтожение,  
изменение**

**нарушение  
доступности**

**блокирование**

## Съем информации с ВОЛС

---

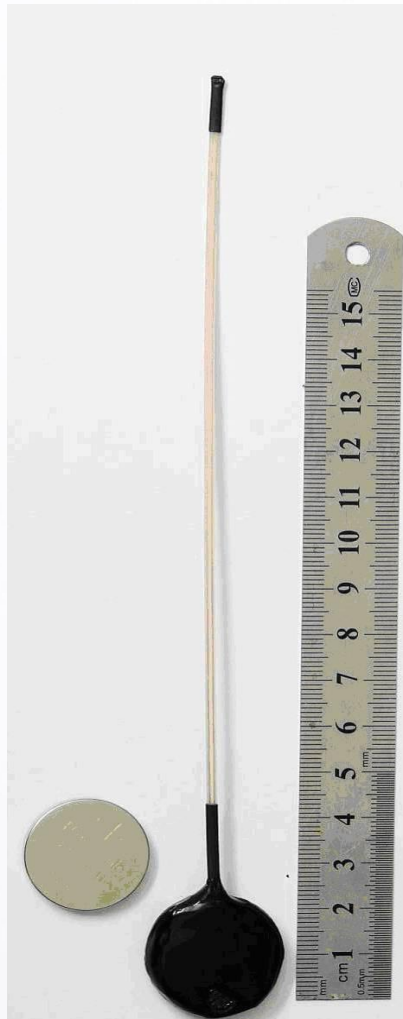
**Подключение с  
кратковременным  
разрывом ВОЛС**



**Подключение к работающему  
каналу ВОЛС без разрыва  
соединения**



# Радиомикрофон аналоговый NFM-400M (BT3V-300)



- частота: 400-470 МГц
- питание: батарея CR2450
- время работы: 100-120 ч
- дальность : 300-400 м

## Преимущества:

- большое время работы и быстрый запуск
- большой радиус передачи
- защита аудио тракта от громких ударов и хлопков
- высокая проходимость сигнала через препятствия, за счёт применения сравнительно низких частот;
- сравнительно высокая скрытность работы, за счёт применения очень точной частоты работы передатчика и не высокой средней мощности сигнала.

## Недостатки:

- сравнительно длинная антенна 15-17см

# Радиомикрофон аналоговый WFM-1G(VN-120)

- частота: 900 - 1100 МГц
- питание: батарея любая на 3-6 V
- время работы: от батареи CR2450 до 40-50 ч
- дальность работы при прямой видимости: 100-150м
- **Преимущества:**

- минимальные шумы в эфире
- короткая антенна 6.5-7см

## **Недостатки:**

- хуже проходимость сигнала через препятствия (по сравнению с частотами 400-470;600-670MHz)
- повышенное энергопотребление при сравнительно не большой дальности





# Цифровой радиомикрофон MP-04

- дальность действия: 300 м
- чувствительность встроенного микрофона: 7-9 М
- питание: 3 V
- габариты: 30X40X7 мм
- рабочая частота: 410-440 МГц
- источник питания: один элемент CR2450



# Радиомикрофон MP2



- дальность - до 3 км
- питание - 9В
- время работы до 4 дней
- габариты - 30 X 12X 8 мм.
- частота - 96,1М гц (частота передатчика регулируемая)

# Пример закладного устройства негласного съема информации («Златоуст»)



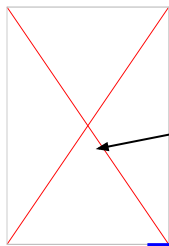
Генри Кэбот Лодж, представитель США в ООН, демонстрирует «Златоуста» во время чрезвычайной сессии Организации Объединенных Наций. В настоящее время он хранится в музее ЦРУ в Лэнгли.

# Видеонаблюдение за помещением с использованием телевизионной камеры, установленной на беспилотном дистанционно – управляемом вертолете (БПВ)

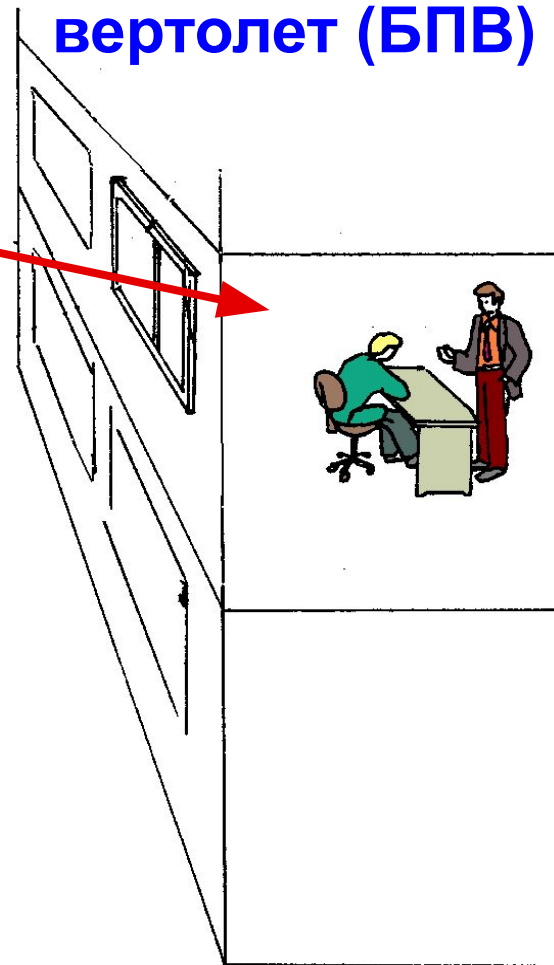


**Телевизионная камера**

**Малогобаритный беспилотный вертолет (БПВ)**



**Пульт дистанционного управления БПВ**



# Беспилотный малогабаритный вертолет с электрическим малошумным двигателем SkyEye

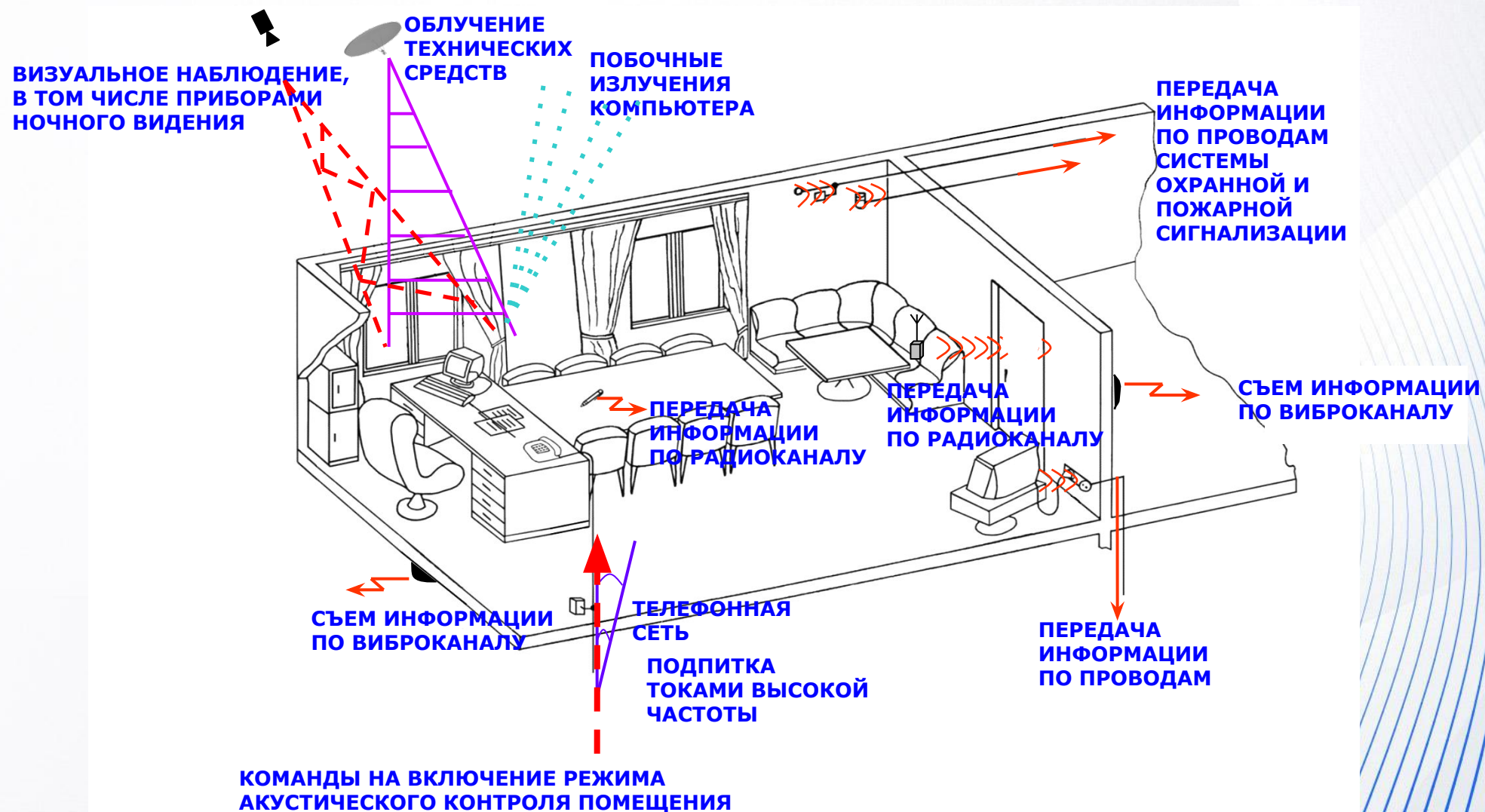
Уровень шума 65 дБ  
на расстоянии 3 м



## Беспилотный управляемый вертолет SIM-SkyEye



# Технические каналы утечки информации из офисного помещения



# Нормативно-правовое обеспечение (обзорно для ОУ)

---

1. Конституция РФ.
2. ФЗ-152 «О персональных данных».
3. ФЗ-149 «Об информации, информационных технологиях и о защите информации».
4. Требования по защите коммерческой тайны (98-ФЗ)
5. Требования по защите инсайдерской информации (224-ФЗ)
6. Требования по защите данных в Национальной платежной системе (161-ФЗ, ПП-584, 382-П и другие)
7. Приказ ФСТЭК России №17, №21, Постановление Правительства РФ №1119, Методические рекомендации ФСТЭК России
8. Требования по защите информации в АСУ ТП (Приказ ФСТЭК России №31)
9. Требования к безопасности данных индустрии платежных карт - PCI DSS
10. СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»
11. РС БР ИББС-2.9-2016 «Предотвращение утечек информации»
12. Комплексный международный стандарт по информационной безопасности ISO 27001
13. Международные нормативно-правовые акты и стандарты (Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act of 2002 и т.д.)



# Информационные ресурсы федеральных регуляторов безопасности информации и нормативно-правового обеспечения ИБ

---

- <http://www.fstec.ru>
- <http://www.fsb.ru>
- <http://www.rsoc.ru>
- <http://www.garant.ru>
- <http://www.consultant.ru>
- <http://www.gost.ru/wps/portal>
- <http://www.abiss.ru/doc>

---

**Спасибо за внимание!**