



ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ

Государственное бюджетное профессиональное образовательное учреждение г. Москвы Колледж связи № 54 им. П.М.Вострухина

ЛАБОРАТОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*"БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ"*

РАЗДЕЛ I. Основы безопасности информационных технологий Тема 2. Основные понятия в области безопасности информационных технологий

МОСКВА 2016





**ЧТО ТАКОЕ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ?**

**ОТ ЧЕГО (ОТ КОГО) ЗАЩИЩАТЬ?**



**ЧТО (КОГО) ЗАЩИЩАТЬ?**

**ЗАЧЕМ ЗАЩИЩАТЬ?**

**КАК И КАКИМИ СРЕДСТВАМИ ЗАЩИЩАТЬ?**





**Автоматизированная система** – организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов:

★ **Технические средства обработки и передачи данных** (средств вычислительной техники и связи)



★ **Методы и алгоритмы обработки данных** в виде программного обеспечения



★ **Информация** (массивы, базы данных) на различных носителях



★ **Обслуживающий персонал и пользователи системы**





**Информация** – сведения о фактах, событиях, процессах и явлениях, о состоянии объектов (об их свойствах и характеристиках) в некоей предметной области, необходимые для оптимизации принимаемых решений в процессе управления этими объектами.

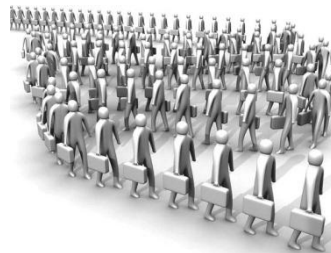
**Информационные ресурсы** – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).



**Обработка информации в АС** – любая совокупность операций (прием, накопление, хранение, преобразование, отображение, передача и т.п.), осуществляемых над информацией (сведениями, данными) с использованием средств АС.



**ОБЩЕСТВЕННЫЕ  
ИЛИ КОММЕРЧЕСКИЕ  
ОРГАНИЗАЦИИ И  
ПРЕДПРИЯТИЯ**  
**(юридические лица)**



**ОТДЕЛЬНЫЕ ГРАЖДАНЕ**  
**(физические лица)**

**ГОСУДАРСТВО**

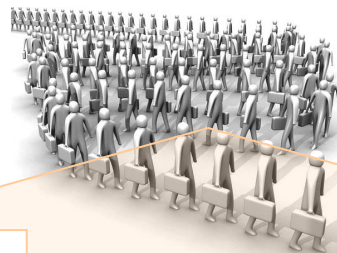
(в целом или отдельные  
его ведомства, органы  
и организации)



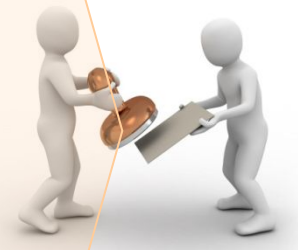
*Субъекты информационных отношений*



# Роли субъектов информационных отношений



1. Источники (поставщики) информации;
2. Потребители (пользователи) информации;
3. Собственники, владельцы, обладатели, распорядители;
4. Физические и юридические лица о которых собирается информация;
5. Участники процессов обработки и передачи информации









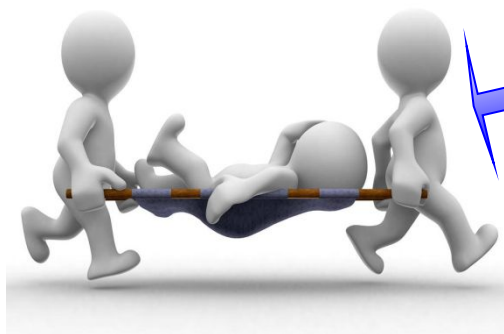
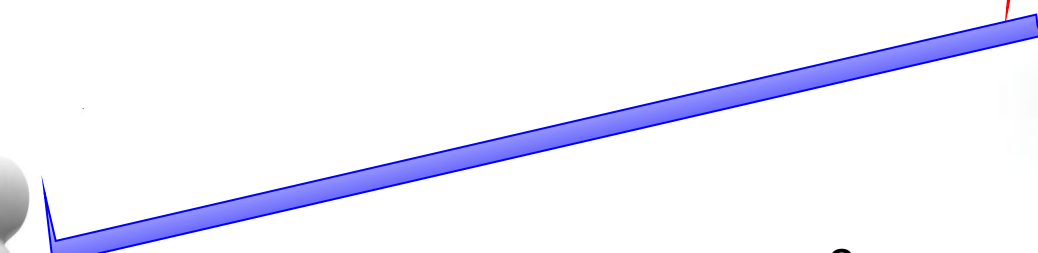
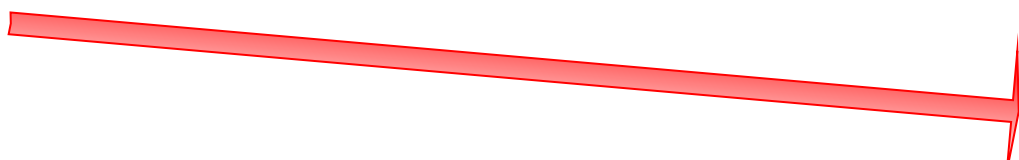
## Субъекты информационных отношений



Будучи заинтересованным хотя бы в одном из вышеуказанных свойств, **субъект информационных отношений:**



является **УЯЗВИМЫМ**



Заинтересован в своей **ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**



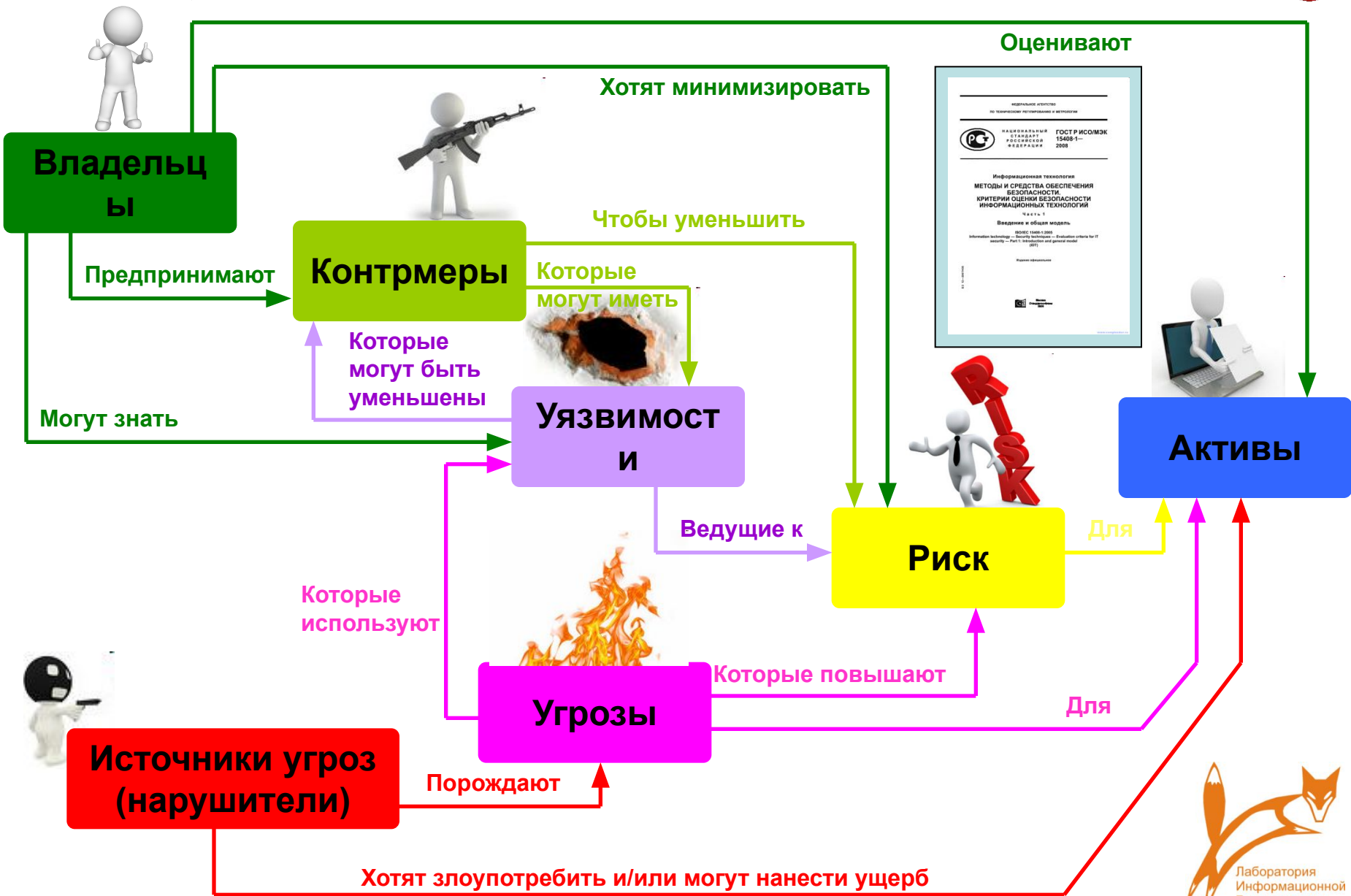
Потенциально подвержен **УЩЕРБУ**  
(прямому или косвенному, моральному  
или материальному)







# Понятия безопасности и их взаимосвязь ГОСТ Р ИСО/МЭК 15408-1-2008

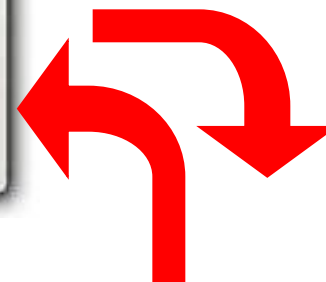
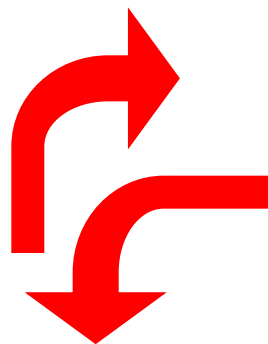




# Необходимость обеспечения (защиты) свойств информации



Конфиденциальность информации



Целостность информации



Доступность информации





# Необходимость обеспечения (защиты) свойств информации



1. Информация конфиденциальна и целостна, значит она точно никому не доступна;
2. Информация конфиденциальна и всем доступна, значит она точно уже не целостна;
3. Информация целостна и всем доступна, значит она точно уже не конфиденциальна.





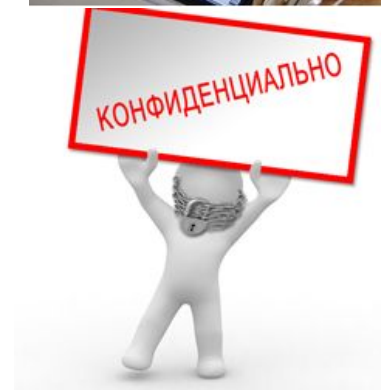
**Доступность информации** – такое свойство системы (средств и технологий обработки), которое характеризует способность обеспечивать своевременный доступ субъектов к интересующей их информации и соответствующим автоматизированным службам всегда, когда в обращении к ним возникает необходимость.





**Целостность информации** – такое свойство информации, которое заключается в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

**Конфиденциальность информации** – характеристика, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (инфраструктуры) сохранять указанную информацию в тайне от субъектов, не имеющих прав на доступ к ней.





Защищенность информации от нежелательного для соответствующих субъектов информационных отношений ее разглашения (нарушения **конфиденциальности**), искажения или утраты (нарушения **целостности**) или снижения степени **доступности** (блокирования) информации, а также незаконного ее тиражирования (неправомерного использования).



Безопасность информации





## Безопасность автоматизированной системы

– защищенность всех ее КОМПОНЕНТОВ:



технических  
средств



программного  
обеспечения



```
sp0: (Generic ISD U0B) at port 0x3c0-0x3d1 Iomem 0x0000-0xbffff on isa0  
fireconster "TSC" frequency 1066200140 Hz quality 000  
fireconsters tick every 10 000 nsec  
setting 5 seconds for SCSI devices to settle  
sdhci: 120Mbps Full Speed USB v2.0  
usb1: 480Mbps High Speed USB v2.0  
cdrom: CDROM (QEmu Virtual IDE CDROM Drive/000000001) at ata-master UDMA33  
scsi1: (ata) at usb0  
hub0: (Intel UHCI root HUB, class 9/0, rev 1.00/1.00, addr 1) on usb0  
scsi1: (ata) at usb0  
hub1: (48x15nd) EHCI root HUB, class 9/0, rev 2.00/1.00, addr 1) on usb0  
scsi1: (ata) at usb0  
hub1: 6 ports with 6 removable, self powered  
cdrom at spt0 bus 0 target 0 lun 0  
scsi1: (QEmu, QEmu Virtual) 2.1-0 Fixed Direct Access SCSI-2 device  
sd: 320.000MB/s transfers (160.000MB/s DT, offset 127, 16bit)  
sd: Command Queuing enabled  
sd: 10240MB (20971520 512 byte sectors: 25M 63K-T 1385C)  
trying to mount root from sfs:/dev/sd0  
scsi1: Version 0.3.0-pre1, FUSE ABI 7.0  
-----  
rooting R-Studio Agent Emergency. Please wait...  
setting 0 seconds for PCMCIA devices to settle...  
rooting R-Studio Agent Emergency. Now you may remove floppy.
```

данных



пользователей  
и персонала

от разного рода нежелательных для соответствующих субъектов воздействий.



## Цель обеспечения безопасности автоматизированной системы

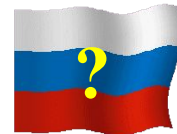
– защита всех категорий субъектов (как внешних, так и внутренних), прямо или косвенно участвующих в процессах информационного воздействия, от нанесения им ощутимого материального, морального или иного ущерба в результате случайных или преднамеренных нежелательных воздействий на информацию и системы ее обработки и передачи



**Цель защиты циркулирующей в АС информации** – предотвращение разглашения (утечки), искажения (модификации), утраты, блокирования (снижения степени доступности) или незаконного тиражирования информации



## Контрольные вопросы



### Контрольные вопросы:

1. Дайте определение автоматизированной системы.
2. Что такое информация?
3. Что включают в себя информационные ресурсы?
4. Назовите субъекты информационных отношений.
5. Каковы роли субъектов информационных отношений?
6. Раскройте понятие безопасности и их взаимосвязь в соответствии с ГОСТ Р ИСО/МЭК 15408-1-2008.
7. Что в себя включают понятия целостности, конфиденциальности и доступности информации?
8. Дайте определение безопасности информации.
9. Что включает в себя понятие безопасности информационной системы?
10. Что является целью обеспечения безопасности автоматизированной системы?





ГБОУ СПО КОЛЛЕДЖ СВЯЗИ № 54



**Спасибо за внимание!**



Лаборатория  
Информационной  
Безопасности