РОССИЙСКИЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Г.В. ПЛЕХАНОВА

# Лекция:

## Концептуальные основы информационной безопасности

Доцент кафедры прикладной информатики и информационной безопасности к.т.н., доцент Карпов Д.С.

## Учебные вопросы

1. Основы системного понимания информационной безопасности

2. Современная постановка задачи обеспечения информационной безопасности

# Перечень основных нормативно-правовых актов в области ИБ

1. **Конституция Российской Федерации от 25.12.1993 г.**
2. **Стратегия национальной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 31.12.2015 N 683).**
3. Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы (утверждена Указом Президента РФ от 9 мая 2017 г. № 203).
4. **Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.).**
5. **Основные направления научных исследований в области обеспечения информационной безопасности РФ (утв. Секр. Совета Безопасности РФ Н.П. Патрушевым 31 августа 2017 г.)**
6. Программа "Цифровая экономика Российской Федерации". Утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. N 1632-р
7. **Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».**
8. Федеральный закон от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»
9. Федеральный закон от 28.12.2010 г. № 390-ФЗ «О безопасности».
10. **Закон РФ от 21.07.1993 г. № 5485-1 «О государственной тайне».**
11. **Федеральный закон от 29.07.2004 г. N 98-ФЗ «О коммерческой тайне».**
12. **Федеральный закон РФ 27.07.2006 г. N 152-ФЗ «О персональных данных».**
13. Федеральный закон от 3.04.1995 г. N 40-ФЗ «О Федеральной службе безопасности».
14. Федеральный закон от 07.02.2011 N 3-ФЗ «О полиции».
15. Федеральный закон от 28.12. 2010 г. N 403-ФЗ «О следственном комитете Российской Федерации».
16. **Кодекс Российской Федерации об административных правонарушениях (№ 195-ФЗ от 30 декабря 2001 года).**
17. **Трудовой кодекс Российской Федерации от 30.12.2001 г. N 197-ФЗ.**
18. **Уголовный кодекс Российской Федерации (№ 63-ФЗ от 13 июня 1996 года).**

# Перечень основных нормативно-правовых актов в области информационной безопасности

19. Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
20. Указ Президента РФ от 03 апреля 1995 N 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».
21. Указ Президента РФ № 960 от 11 августа 2003 г. «Вопросы Федеральной службы безопасности Российской Федерации».
22. Указ Президента РФ от 16 августа 2004 года № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
23. **Указ Президента РФ от 06.03.1997 N 188 «Об утверждении Перечня сведений конфиденциального характера»**.
24. **Пост. Пр-ва РСФСР от 05.12.1991 N 35 «О перечне сведений, которые не могут составлять коммерческую тайну».**
25. **Пост. Пр-ва РФ от 03.11.1994 N 1233 «Об утв. Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».**
26. Пост. Пр-ва РФ от 22.09.2009 N 754 «Об утверждении Положения о системе межведомственного электронного документооборота».
27. Распоряжение Пр-ва РФ от 02.10.2009 N 1403-р «О технических требованиях к организации взаимодействия системы межведомственного документооборота с системами электронного документооборота федеральных органов исполнительной власти».
28. Пост. Пр-ва РФ от 26.06.1995 N 608 «О сертификации средств защиты информации».

# Перечень основных нормативно-правовых актов в области ИБ

**29. Приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»**

**30. Приказ ФСТЭК России от 18 февраля 2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных».**

31. Положение о сертификации средств защиты информации по требованиям безопасности информации. Утверждено Приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 г. N 199.

32. Положение по аттестации объектов информатизации по требованиям безопасности информации Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.

33. Приказ ФСТЭК России от «10» апреля 2015 г. № 33 «Об утверждении Правил выполнения отдельных работ по аккредитации органов по сертификации и испытательных лабораторий, выполняющих работы по оценке (подтверждению) соответствия в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, в установленной ФСТЭК России сфере деятельности».

34. Приказ ФСБ России от 11 апреля 2014 г. № 202 «Об утверждении административного регламента ФСБ РФ по предоставлению государственной услуги по лицензированию деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»

35. Приказ ФСБ России от 23 марта 2016 года № 185 «Об утверждении Административного регламента ФСБ РФ по исполнению государственной функции по осуществлению лицензионного контроля деятельности по разработке и производству средств защиты конфиденциальной информации».

# Перечень основных нормативных актов в области ИБ

**36. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения**

**37. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения**

**38. Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения**

39. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

40. ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения

41. ГОСТ Р 53113.2-2009 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов

42. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности

43. **ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология**

44. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

45. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента безопасности

46. ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности



47. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

# 1. Основы системного понимания информационной безопасности

# Актуальность темы занятия

Современный мир совершает переход из XX - «энергетического» века в XXI век, который со всей определенностью можно назвать «информационным».

На смену индустриальному этапу общественного развития* приходит эволюционная фаза, названная информатизацией.

Информация как предмет труда становится все в большей степени стратегическим ресурсом общества, движущей производительной силой.

Современные информационные технологии приобретают глобальный характер, охватывая все сферы жизнедеятельности человека, формируя информационное единство всей человеческой цивилизации

Ход всех значимых событий в науке, коммерции, социуме связан с процессами производства и владения информацией.

**Информационная безопасность** - сравнительно молодая, быстро развивающаяся область информационных технологий, теоретико-методологическую основу которой составляют различные области научного знания.

*Индустриализация — процесс ускоренного социально-экономического перехода от традиционного этапа развития к индустриальному, с преобладанием промышленного производства в экономике. Этот процесс связан с развитием новых технологий, особенно в таких отраслях, как энергетика и металлургия. В ходе индустриализации общество также претерпевает некоторые изменения, меняется его мировосприятие.

*Производительные силы - средства производства ( орудия труда и предметы труда), с помощью которых производят материальные блага (осуществляют материальное производство ), а также люди, способные к труду, имеют определенные навыки и знания и приводят в действие эти средства и совершенствуют их.

# Возрастание роли информационно-технической борьбы

В военном деле наступает новый, постядерный этап развития.

Эффективность современного оружия все больше определяется не столько огневой мощью, сколько степенью информационной обеспеченности. Информатизация армии стала приоритетной задачей военно-технической политики государства. В содержании военных действий значительно возросла значимость информационно-технического противоборства.

Возрастание роли информационно-технической борьбы стирает границу между войной и миром. Вооруженные силы ряда государств находятся в постоянном информационном противоборстве, а **военная информатика** и в мирное время решает задачи, характерные для войны.

Роль информационной войны сегодня осознается российским руководством. В выступлении вице-премьера Д. Рогозина в «РГ» 28 июня 2013 года, говорится следующее: **«Если раньше все военные наработки в этой сфере [кибероружия] затрагивали лишь обеспечение безопасности компьютерных систем и коммуникаций, то теперь информационные технологии рассматриваются как оружие первого удара. В случае конфликта с каким-либо государством, возможная первая атака производится через информационные сети, в ходе которой разрушаются критически важные объекты инфраструктуры государства, нарушается система политического и военного управления, выключаются станки с электромозгами, основанными на импортной электронно-компонентной базе. Когда же государство-жертва агрессии становится практически парализованным, наносится удар классическими военными средствами»**.

Пресс-секретарь Президента РФ Д. Песков (в программе «Право знать» на «ТВЦ», в 2016 г.) заявил: «**Сейчас мы находимся в состоянии информационной войны с законодателями моды в информационном пространстве, прежде всего, с англосаксами, их СМИ**».

**"Мы — в состоянии информационной войны**, — констатировала Хиллари Клинтон. — **Во время "холодной войны", мы невероятно преуспели в том, чтобы донести голос Америки. Но после падения Берлинской стены, мы решили – «Все, хватит, дело сделано" – и, к сожалению, мы теперь серьезно расплачиваемся за это»** (2016 г.).

# Возрастание роли информационно-технической борьбы

В Пентагоне руководствуются лозунгом «Радиоэлектронная война никем в не объявляется, никогда не прекращается, ведется скрытно и не знает границ пространстве и времени».

С 1992 г. термин «информационная война» стал официально использоваться в руководящих документах министерства обороны США, а в 1996 г. Пентагон утвердил доктрину информационной войны под названием «Доктрина войны с системами боевого управления».

Американские военные представляют реализацию концепции информационной войны следующим образом.

Некий «диктаторский режим» угрожает одному из союзников Соединенных Штатов. Вместо того чтобы направить в этот регион тысячи солдат и десятки боевых кораблей, США обрушивают на диктатора множество бед, созданных при помощи компьютера. Сперва с помощью агентов в телефонную сеть страны внедряется компьютерный вирус, который приводит к почти полному выводу из строя телефонной связи. Вводятся также специальные микробы, вызывающие поражение физической основы электронной аппаратуры. Затем компьютерные логические бомбы, установленные на определенное время «подрыва», разрушают электронные устройства, управляющие движением воздушного и железнодорожного транспорта. Они нарушают график и меняют направления полетов самолетов и движения поездов, создают предпосылки катастроф на земле и в воздухе. Войска специального назначения проникают на территорию столицы противника и активируют неядерные устройства, вызывающие мощный электромагнитный импульс (ЭМИ). В результате подрыва таких устройств, скажем, вблизи центрального банка, биржи в этих учреждениях выходят из строя все компьютеры и информационные системы, парализуется финансовая жизнь страны. Между тем командирам воинских формирований противника по информационным системам и радиосредствам передаются ложные приказы. Войска, разбросанные на огромных пространствах, теряют боеспособность. Самолеты ВВС США, специально оборудованные для проведения психологических операций, глушат передачи правительственного телевидения, заменяя их созданными с помощью компьютеров передачами, в которых агрессивный лидер делает вызывающие отрицательную реакцию заявления, что приводит к утрате им поддержки населения. А вскоре диктатор или люди из его окружения обнаруживают, что деньги, положенные на счета в иностранных банках, пропали бесследно…

*Источник: http://www.modernarmy.ru/article/282/informacionnaya-voina Портал "Современная армия"*

# Возрастание роли информационно-технической борьбы

В 1998 г. МО США была разработана новая «Объединенная доктрина информационных операций». В ней впервые вводится термин «стратегическое информационное противоборство».

Целями воздействия в нем являются объекты противника, выбираемые по принципу «пяти колец» (по мере убывания важности): политическое и военное руководство страны; системы жизнеобеспечения; инфраструктура; население; вооруженные силы.

Поскольку воздействие на указанные объекты осуществляется с помощью сетевых технологий и методов, такое противоборство получило название «информационно-сетевая война».

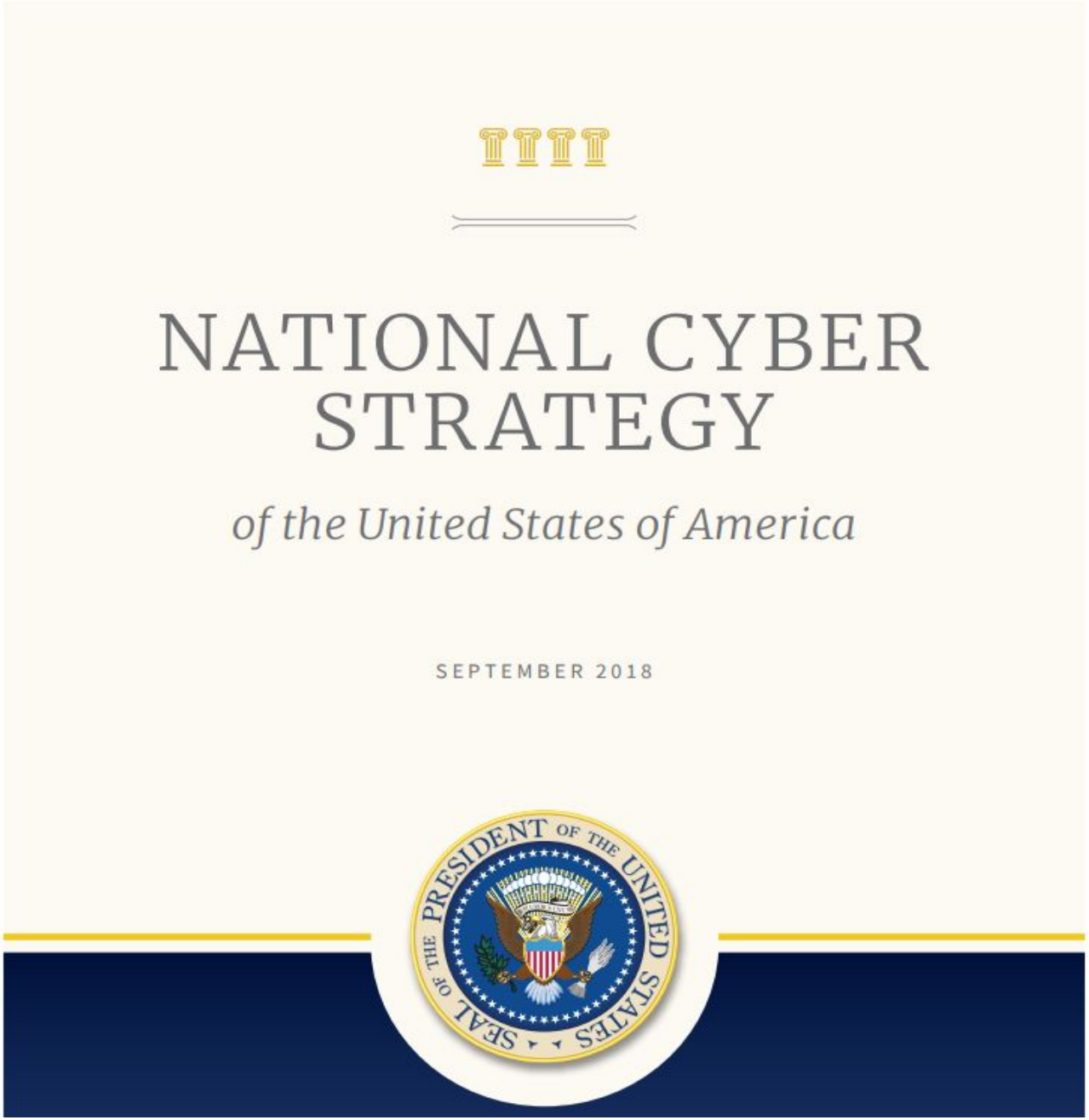
Основой ее является массированное воздействие на морально-психологическое состояние руководство и население страны-противника. Причем, зачастую даже сам факт такого воздействия заблаговременно не может быть выявлен ее спецслужбами.

Информационно-сетевая война предусматривает проведение комплекса мероприятий в отношении противника:

- создание атмосферы бездуховности и безнравственности, что автоматически создает благоприятную атмосферу для нагнетания конфликтной обстановки внутри страны-противника и падению авторитета государственной власти;
- манипулирование общественным мнением и политической ориентацией социальных групп с целью создания обстановки политической напряженности и хаоса;
- дестабилизация политических отношений между партиями, объединениями и движениями с целью провокации конфликтов, разжигания атмосферы недоверия и подозрительности;
- обострение политической борьбы, провоцирование репрессий против оппозиции; развязывание в обществе гражданской войны;
- снижение уровня информационного обеспечения органов власти и управления с целью затруднения принятия важных решений;
- дезинформация населения о работе государственных органов, подрыв их авторитета, дискредитация органов управления; провоцирование социальных, политических, национальных и религиозных столкновений;
- инициирование массовых протестных акций, забастовок, массовых беспорядков; подрыв международного авторитета государства; нанесение ущерба жизненно важным интересам государства в политической, экономической, оборонной и других сферах.

*Источник: http://www.modernarmy.ru/article/282/informacionnaya-voina Портал "Современная армия"*

# Стратегия США в киберпространстве (2018 г.)



# Стратегия США в киберпространстве (2018 г.)

«**Наши руки больше не связаны**»

Новая стратегия США в киберпространстве декларирует более жесткий подход к соперникам страны на этом направлении. «**Мы не будем задействовать только оборонные меры, мы намерены участвовать в наступательных операциях, и наши соперники должны иметь это в виду**», — подчеркнул помощник президента США по национальной безопасности Джон Болтон (цитата по CNN), анонсируя стратегию 20 сентября 2018 г. В числе соперников Америки в киберпространстве в документе упомянуты Россия, Северная Корея, Иран и Китай. Незасекреченная 40-страничная версия стратегии опубликована на сайте Белого дома.

Как обратил внимание Болтон, **президент Дональд Трамп расширил полномочия киберкомандования США, позволив ему проводить превентивные и наступательные операции в отношении враждебных государств**. «**Наши руки больше не связаны в отличие от [администрации] Обамы**», — сказал помощник американского лидера. В 2012 году администрация Барака Обамы приняла указ, ограничивающий возможности для проведения масштабных кибероперациий без предварительных межведомственных консультаций.

Новая **стратегия позволит США достичь «критически важных целей в сфере безопасности, а также поможет процветанию Америки, защищая мир посредством использования силы**», прокомментировал публикацию документа Трамп. **«Америка создала интернет и поделилась им с остальным миром, теперь мы должны сделать все необходимое, чтобы сохранить <...> киберпространство для следующих поколений»**, — говорится в заявлении президента.

Анонсированный 20 сентября план действий — «первая четкая киберстратегия Соединенных Штатов за 15 лет», напомнил Трамп. Первая подобная доктрина была принята в 2003 году и называлась «Национальная стратегия по защите киберпространства».

Новая киберстратегия США предполагает активизацию усилий на 4-х основных направлениях:

- укрепление национальной безопасности: защита сетей, систем и данных;
- помощь процветанию Америки путем создания безопасной и растущей цифровой экономики, а также через развитие инноваций внутри страны;
- сохранение мира и процветания путем укрепления способности США и их партнеров предотвращать и в случае необходимости наказывать тех, кто использует киберинструменты в целях агрессии;
- наращивание влияния за пределами США, расширение зоны открытого и надежного интернета.

# Возрастание роли информационно-технической борьбы

**Как США собираются доминировать в интернете**

Хотя текст стратегии не содержит деталей, там тем не менее обозначены основные контуры реализации поставленных Белым домом целей. Для укрепления национальной безопасности и развития экономики США намерены, во-первых, **добиться более централизованного и слаженного процесса принятия решений в киберсфере на федеральном уровне и, во-вторых, продолжать укреплять системы защиты от киберугроз**.

**Чтобы развивать цифровую экономику, Белый дом считает необходимым наращивать инвестиции в новые инфраструктурные проекты. Речь идет, в частности, о развитии технологий сети 5G и поощрении новых разработок в области ИТ**.

**Бороться с враждебными действиями других стран и транснациональных хакерских группировок Вашингтон планирует путем выявления и передачи Соединенным Штатам большего числа иностранных киберпреступников. Вашингтон и союзники также собираются выработать процедуры, позволяющие быстро реагировать и отвечать на атаки противников в цифровом пространстве,** сообщается в стратегии Белого дома. Для борьбы с «враждебными акторами» США готовы использовать также военные, экономические и дипломатические меры воздействия, подчеркивается в документе.

Упоминается в новой стратегии и угроза информационных кампаний. «**Соединенные Штаты будут использовать соответствующие инструменты на национальном уровне, чтобы выявлять и бороться с вредоносным влиянием, которое несут информационные онлайн-кампании**», — утверждается в документе. В ноябре 2017 года американский конгресс обвинял Россию в попытках манипулировать общественным мнением в США через соцсети, в том числе в период президентских выборов. По мнению американских политиков, Москва пытается усугубить политический раскол в США и таким образом ослабить доверие граждан страны к институтам власти.

https://www.rbc.ru/newspaper/2018/09/24/5ba4d2459a79475744112262

# Основные внешние информационные угрозы РФ

Основные внешние информационные угрозы и состояние информационной безопасности (сформулированы в Доктрине информационной безопасности, утв. Указом Президента РФ № 646 от 5 декабря 2016 г.)

1. Одним из основных негативных факторов, влияющих на состояние информационной безопасности, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.

Одновременно с этим усиливается деятельность организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.

2. Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий.

Отмечается тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации. Российские средства массовой информации зачастую подвергаются за рубежом откровенной дискриминации, российским журналистам создаются препятствия для осуществления их профессиональной деятельности.

Наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.

# Основные внешние информационные угрозы РФ

3. Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

4. Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.

5. Постоянно повышается сложность, увеличиваются масштабы и растет скоординированность компьютерных атак на объекты критической информационной инфраструктуры, усиливается разведывательная деятельность иностранных государств в отношении Российской Федерации, а также нарастают угрозы применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации.

6. Существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети «Интернет», не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими.

# Стратегические цели и основные направления обеспечения информационной безопасности

**20. Стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.**

21. В соответствии с военной политикой Российской Федерации основными направлениями обеспечения информационной безопасности в области обороны страны являются:

а) **стратегическое сдерживание и предотвращение военных конфликтов**, которые могут возникнуть в результате применения информационных технологий;

б) **совершенствование системы обеспечения информационной безопасности** Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства;

в) **прогнозирование, обнаружение и оценка информационных угроз**, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере;

г) **содействие обеспечению защиты интересов союзников Российской Федерации** в информационной сфере;

д) **нейтрализация информационно-психологического воздействия**, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества.

**Определены также стратегические цели обеспечения ИБ в экономической сфере, в области государственной и общественной безопасности, науки, технологий и образования, стратегической стабильности и равноправного стратегического партнерства.**

# Основные внутренние угрозы для РФ в информационной сфере

**Отсутствие четко сформулированной информационной политики, отвечающей национальным целям, ценностям и интересам:**

- заявленный в Конституции РФ приоритет интересов личности и общества нередко подменяется в законах приоритетом интересов ведомств, законодательство субъектов федерации зачастую не соответствует федеральному уровню, а подзаконные акты по-прежнему являются основой для произвола чиновников;

- несовершенство единой системы отбора информации, подготовки и принятия эффективных решений на высшем уровне;

- отсутствие должного взаимодействия между существующими структурами обеспечения безопасности, когда ведомства порой подменяют государственные интересы узковедомственными и вступают в противостояние в борьбе за усиление своих полномочий;

- отсутствие системы эффективного контроля за обеспечением безопасности как со стороны вышестоящих государственных структур, так и со стороны общества и граждан, в силу чего нередко даже правильные и необходимые решения не выполняются.

# «Кто владеет информацией, тот владеет миром»

В современном мире, когда формируется и развивается информационное общество, когда разворачивается глобальная информационная война афоризм «кто владеет информацией, тот владеет миром»* является не менее актуальным.

Успех военных действий на суше, в воздухе и на море, в равной степени, как и предотвращение войны, военно-политических кризисов или вооруженных конфликтов существенно зависят от эффективности использования разведывательной и, в частности, аэрокосмической информации.

Линдон Б. Джонсон (36-й Президент США от Демократической партии с 22 ноября 1963 года по 20 января 1969 года): «Римская империя контролировала мир потому, что сумела построить дороги. Затем, когда началось освоение морских пространств, Британская империя доминировала в мире, так как имела корабли. В век авиации мы были могущественны, поскольку имели в своем распоряжении самолеты. Сейчас коммунисты захватили плацдарм в космосе».

Это убедительно говорит в пользу использования результатов разведывательной, в частности аэрокосмической деятельности, в интересах обеспечения национальной безопасности, а также ее основных составных частей: военной, информационной, экологической и др. безопасности государства.

*Натан Ротшильд — основатель английской ветви династии Ротшильдов. В 1815 году вся Европа с тревогой ждала, чем закончится решающая битва между армиями Наполеона и Веллингтона при Ватерлоо. В начале сражения наблюдателям показалось, что выигрывает Наполеон, о чем срочно сообщили в Лондон. Однако, на помощь войскам Веллингтона подоспел прусский корпус и решил исход боя в пользу союзников. Наполеон бежал.

Утром следующего дня Натан Ротшильд явился на Лондонскую биржу. Он был единственным в Лондоне, кто достоверно знал о поражении Наполеона. Сокрушаясь по поводу успехов Наполеона, он немедленно приступил к массовой продаже своих акций. Все остальные биржевики сразу же последовали его примеру, так как решили, что сражение проиграли англичане. Поднялась паника. Английские, австрийские и прусские ценные бумаги дешевели с каждой минутой. Лондонская биржа буквально ломилась от обесцененных акций. Их тайно и спешно скупали подставные агенты Ротшильда.

О том, что Наполеон проиграл битву, на бирже узнали лишь через день. Многие держатели ценных бумаг покончили с собой, а Натан за один день заработал 40 миллионов фунтов стерлингов и овладел большой долей британской экономики. Такую же операцию на Парижской бирже осуществил брат Натана Ротшильда Якоб.

# «Кто владеет информацией, тот владеет миром»

## Кодекс Ротшильдов

**1. Все важные посты в бизнесе должны занимать только члены семьи (а не наемные работники); участвовать в делах могут только потомки мужского пола; наследовать — только прямые наследники мужского пола. Старший сын становится главой семьи, если братья единодушно не признали иное.**

Так было и в 1812, когда главой дома был утвержден Натан, третий из 5 сыновей Ротшильда.

**2. Мужчины семьи должны жениться на своих двоюродных или троюродных сестрах, чтобы накопленное имущество осталось внутри семьи и служило общему делу. Дочери должны выходить замуж за аристократов, сохраняя свою веру.**

Из 58 браков потомков Меира-Амшеля половина была заключена между двоюродными братьями и сестрами.

**3. В любом случае имущество семьи не описывать, размер состояния не оглашать. Даже в суде или в завещании. Споры между братьями разрешать внутри семьи, сохраняя единство дома.**

Многие исследователи отмечают, что во всех завещаниях баронов присутствуют наставления, зароки, мистика и тайна. «Категорически и самым решительным образом запрещаю проведение судебной или общественной описи моего наследства, любое судебное вмешательство и любое обнародование размеров моего состояния». Такой пункт содержался в завещании французского миллионера Ансельма де Ротшильда.

**4. Никогда не гнаться за непомерно высокой прибылью и оградить себя от любых случайностей, знать во всем меру и никогда не терять цель из виду.**

Сыновья Майера Амшеля Ротшильда так и делали, стараясь вкладываться только в продуманные и солидные долгосрочные проекты, однако бывали и исключения.

**5. Никогда не забывайте, что скромность ведет к богатству!**

Совокупное состояние Ротшильдов, по самым скромным оценкам экспертов, зашкаливает за 3,2 триллиона долларов. Однако точно никто не знает, так как семейство до сих пор старается не раскрывать все свои доходы.

**6. Кто владеет информацией — тот владеет миром!**

Это правило в действии доказали еще пять сыновей Майера Ротшильда, которые хоть и находились в разных концах Европы (старший сын Амшель — во Франкфурте, Натан — в Манчестере, Соломон — в Вене, Карл — в Неаполе, а Джеймс — в Париже), но это лишь способствовало успеху династии, так как глобальная осведомленность позволяла быстро делиться информацией и принимать оптимальные решения. К примеру, во время воин Наполеона Ротшильды подготовили все, чтобы самая свежая информация попадала в первую очередь к ним. Для этого между Франкфуртом, Лондоном и Парижем были открыты станции почтовых лошадей, финансируемые Торговым домом Ротшильдов. Кони Ротшильдов были резвее обычных почтовых, которых «кормили» государственные станционные смотрители. Это помогло семейству финансистов сделать на войне приличное состояние и заставить всю Европу нуждаться в их деньгах.

# Терминология в области информационной безопасности

Информация: Сведения (сообщения, данные) независимо от формы их представления

Данные: Факты, понятия или команды, представленные в формализованном виде и позволяющие осуществлять их передачу или обработку как вручную, так и с помощью средств автоматизации. (Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

В Доктрине информационной безопасности РФ термин *информационная безопасность* используется в *широком смысле*. Это «**состояние защищенности национальных интересов** в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства» (2000 г.);

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 РФ, оборона и безопасность государства (2016 г.).

Термин *информационная безопасность* часто используется в *узком смысле*: *информационная безопасность (information security): сохранение конфиденциальности, целостности и доступности информации.*

*Примечание - Также сюда могут быть включены другие свойства, такие как подлинность, подотчетность, неотказуемость и достоверность (ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология)*

Безопасность информации: Состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность. (ГОСТ Р 50922—2006. "Защита информации. Основные термины и определения").

# Терминология в области информационной безопасности

**Защита информации** - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

(ГОСТ Р 50922—2006. "Защита информации. Основные термины и определения").

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

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

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

(Ст. 16 Федерального закона "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ)

***Таким образом, защита информации - это комплекс мероприятий, направленных на обеспечение безопасности информации и информационной безопасности (часть мероприятий, необходимая, но не достаточная).***

Термин *«компьютерная безопасность»* как эквивалент или заменитель информационной безопасности слишком узок. Компьютеры - только одна из составляющих информационных систем. Информационная безопасность зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал.

# Терминология в области информационной безопасности

## Основные составляющие безопасности информации

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение ***доступности***, ***целостности*** и ***конфиденциальности*** информационных ресурсов и поддерживающей инфраструктуры.

Доступность информации [ресурсов информационной системы]: Состояние информации [ресурсов информационной системы], при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно (Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения).

Иначе говоря - это возможность за приемлемое время получить требуемую информационную услугу.

Целостность: Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право. (ГОСТ Р 50922-2006 Защита информации. Основные термины и определения).

Иначе говоря - это актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность информации: Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. (Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.12.2016) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2017)).

Конфиденциальность (confidentiality): Свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов (ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология)

Иначе говоря - это защита от несанкционированного доступа к информации.

# Модели безопасности

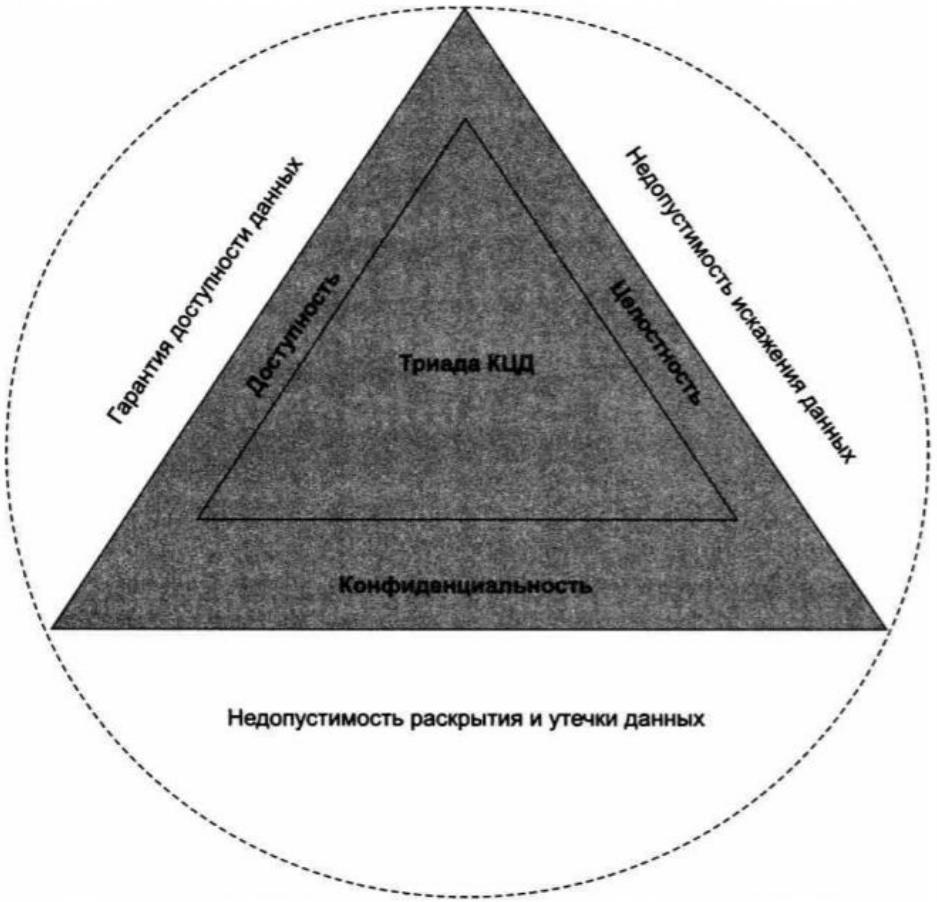


Понятие информационной безопасности может быть пояснено с помощью так называемых **моделей безопасности.**

**Суть этих моделей заключается в следующем: множество всех видов нарушений безопасности делится на несколько базовых групп таким образом, чтобы любое возможное нарушение обязательно можно было отнести по крайней мере к одной из этих групп. Затем система объявляется безопасной, если она способна противостоять каждой из этих групп нарушений.**

Одной из первых и наиболее популярных по сей день моделей безопасности является модель, предложенная Зальцером (Saltzer) и Шредером (Schroeder) (Jerry H. Saltzer, Mike D. Schroeder (September 1975), «The protection of information in computer systems»).

Авторы постулировали, что **все возможные нарушения информационной безопасности всегда могут быть отнесены по меньшей мере к одной из трех групп: нарушения конфиденциальности, нарушения целостности или нарушения доступности.**



# Триада «конфиденциальность, доступность, целостность»



**Информационная система находится в состоянии безопасности, если она защищена от нарушений конфиденциальности, целостности и доступности**, где:

**конфиденциальность** (confidentiality) — это состояние ИС, при котором информационные ресурсы доступны только тем пользователям, которым этот доступ разрешен;

**целостность** (integrity) — это состояние системы, при котором информация, хранящаяся и обрабатываемая этой ИС, а также процедуры обработки информации не могут быть изменены, удалены или дополнены неавторизованным образом;

**доступность** (availability) — это состояние системы, при котором услуги, оказываемые системой, могут гарантированно и с приемлемой задержкой быть предоставлены пользователям, имеющим на это право.

Для ссылки на триаду иногда используют аббревиатуру КЦД (конфиденциальность, целостность, доступность) или в англоязычной форме — CIA.

Требования к безопасности могут меняться в зависимости от назначения информационной системы, характера используемых данных и типа возможных угроз. **Трудно представить систему, для которой нарушения целостности и доступности не представляли бы опасности, вместе с тем обеспечение конфиденциальности не всегда является обязательным**.

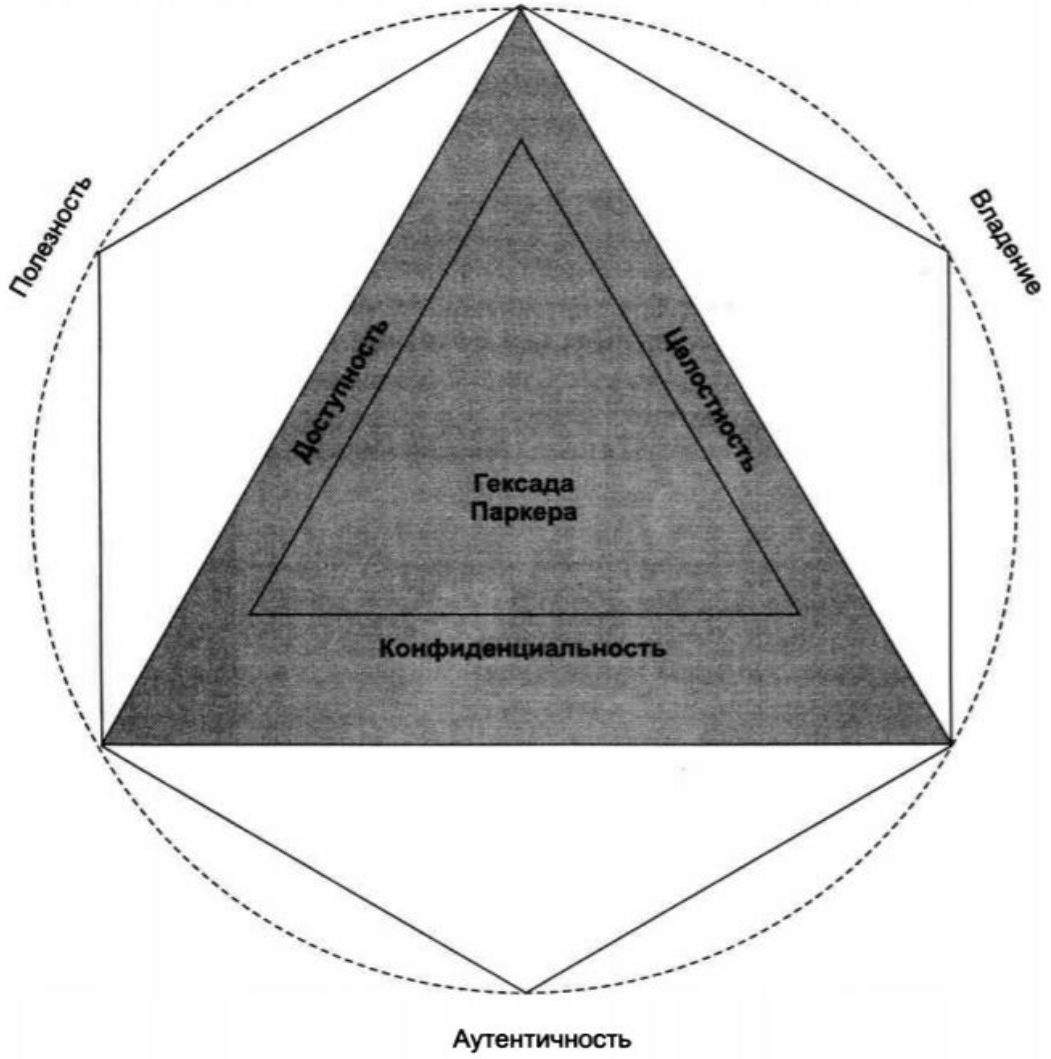
Список свойств безопасной системы следует расширить, добавив к КЦД еще одно свойство — «неотказуемость».

**Неотказуемость** (non-repudiation) — это такое состояние системы, при котором обеспечивается невозможность отрицания пользователем, выполнившим какие-либо действия, факта их выполнения, в частности отрицания отправителем информации факта ее отправления и/или отрицания получателем информации факта ее получения.

# Гексада Паркера и модель STRIDE



Одной из наиболее популярных альтернатив триаде КЦД является так называемая гексада Паркера (Parkerian Hexad) (**Дон Паркер предложил свою гексаду** в работе «Fighting Computer Crime» (1998)), **в которой определено шесть базовых видов нарушений, в число которых, помимо нарушений конфиденциальности, доступности и целостности, входят еще три вида нарушений: аутентичности, владения и полезности**.



# Гексада Паркера и модель STRIDE



**Аутентичность** (authenticity) — это состояние системы, при котором пользователь не может выдать себя за другого, а документ всегда имеет достоверную информацию о его источнике (авторе). Из этого определения видно, что аутентичность является аналогом неотказуемости

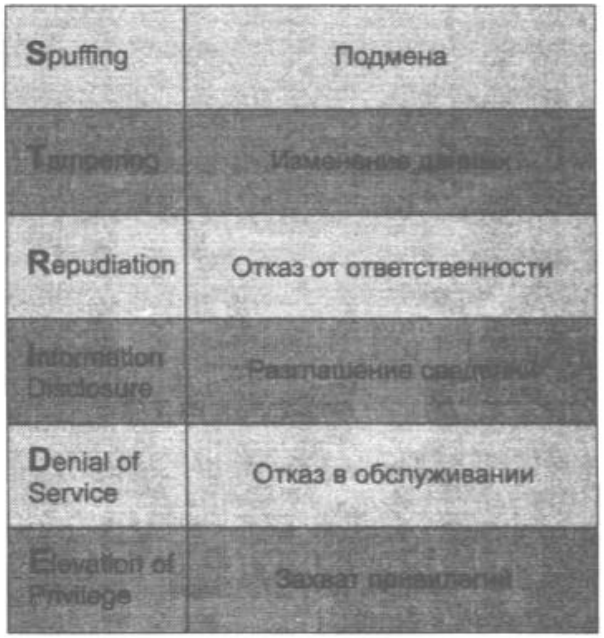
**Владение** (possession) — это состояние системы, при котором физический контроль над устройством или другой средой хранения информации предоставляется только тем, кто имеет на это право

**Полезность** (utility) — это такое состояние ИС, при котором обеспечивается удобство практического использования как собственно информации, так и связанных с ее обработкой и поддержкой процедур. В безопасной системе меры, предпринимаемые для защиты системы, не должны неприемлемо усложнять работу сотрудников, иначе они будут воспринимать их как помеху и пытаться при всякой возможности их обойти.

# Модель STRIDE



Еще одним вариантом определения безопасности ИС является модель STRIDE* (аббревиатура от англоязычных названий типов нарушений безопасности, перечисленных ниже). **В соответствии с этой моделью ИС находится в безопасности, если она защищена от следующих типов нарушений**: подмены данных, изменения, отказа от ответственности, разглашения сведений, отказа в обслуживании, захвата привилегий




*Модель STRIDE используется компанией Microsoft при разработке безопасного программного обеспечения.

**Подмена данных** (spoofing) — это такое нарушение, при котором пользователь или другой субъект ИС путем подмены данных, например IP-адреса отправителя, успешно выдает себя за другого, получая таким образом возможность нанесения вреда системе.

**Изменение** (tampering) означает нарушение целостности.

**Отказ от ответственности** (repudiation) представляет собой негативную форму уже рассмотренного нами свойства неотказуемости (non-repudiation).

**Разглашение сведений** (information disclosure) — это нарушение конфиденциальности.

**Отказ в обслуживании** (denial of service) касается нарушения доступности.

**Захват привилегий** (elevation of privilege) заключается в том, что пользователь или другой субъект ИС несанкционированным образом повышает свои полномочия в системе, в частности незаконное присвоение злоумышленником прав сетевого администратора снимает практически все защитные барьеры на его пути.

# Модель STRIDE



Так же как и в гексаде Паркера, в модели STRIDE все возможное разнообразие нарушений безопасности сводится к шести типам нарушений, три из которых повторяют КЦД (с учетом того, что здесь эти три характеристики безопасности даны в негативном по отношению к КДЦ варианте), однако оставшиеся **три характеристики — подмена данных, отказ от ответственности и захват привилегий — отличают модель STRIDE от гексады Паркера.**

**Российский государственный стандарт** *ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий* **дает определение информационной безопасности на основе гексады Паркера:**

**Информационная безопасность (ИБ) — [это] все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.**

# Системное понимание информационной безопасности


**Объектами** опасного информационного воздействия и, следовательно, **ИБ** могут быть сознание, психика людей, информационно-технические системы различного масштаба и назначения.

**Субъектами ИБ** следует считать те органы и структуры, которые занимаются ее обеспечением.

**Средства обеспечения ИБ** - это средства с помощью которых осуществляются меры по защите информации, систем управления, связи, компьютерных сетей, недопущению подслушивания, маскировке, предотвращению хищения информации и т.д.

**Принципы ИБ**: законность, баланс интересов личности, общества и государства, комплексность, системность, интеграция с международными системами безопасности, экономическая эффективность и т.д.

# Принципы обеспечения информационной безопасности

На основе анализа теоретических и практических аспектов обеспечения компьютерной безопасности **можно выделить ряд общих принципов создания и эксплуатации защищенных компьютерных систем (в которых обеспечивается безопасность информации)**.

**Принцип разумной достаточности.** Внедрение в архитектуру, в алгоритмы и технологии функционирования ИС защитных механизмов, функций и процедур объективно вызывает дополнительные затраты, издержки при создании и эксплуатации, ограничивает, снижает функциональные возможности ИС и параметры ее эффективности (быстродействие, задействуемые ресурсы), вызывает неудобства в работе пользователям ИС, налагает на них дополнительные нагрузки и требования — поэтому защита должна быть разумно достаточной (на минимально необходимом уровне).

**Принцип целенаправленности.** Заключается в том, что применяемые меры по устранению, нейтрализации (либо обеспечению снижения потенциального ущерба) должны быть направлены против перечня угроз (опасностей), характерных для конкретной ИС в конкретных условиях ее создания и эксплуатации.

**Принцип системности.** Выбор и реализация защитных механизмов должны производиться с учетом системной сути ИС, как организационно-технологической человеко-машинной системы, состоящей из взаимосвязанных, составляющих единое целое функциональных, программных, технических, организационно-технологических подсистем.

**Принцип комплексности.** При разработке системы безопасности ИС необходимо использовать защитные механизмы различной и наиболее целесообразной в конкретных условиях природы – программно-алгоритмических, процедурно-технологических, нормативно-организационных, и на всех стадиях жизненного цикла – на этапах создания, эксплуатации и вывода из строя.

# Принципы обеспечения информационной безопасности

**Принцип непрерывности.** Защитные механизмы ИС должны функционировать в любых ситуациях в т. ч. и внештатных, обеспечивая как конфиденциальность, целостность, так и сохранность (правомерную доступность).

**Принцип управляемости.** Подсистема безопасности ИС должна строиться как система управления – объект управления (угрозы безопасности и процедуры функционирования ИС), субъект управления (средства и механизмы защиты), среда функционирования, обратная связь в цикле управления, целевая функция управления (снижение риска от угроз безопасности до требуемого (приемлемого) уровня), контроль эффективности (результативности) функционирования.

**Принцип сочетания унификации и оригинальности.** С одной стороны с учетом опыта создания и применения АИС, опыта обеспечения безопасности ИС должны применяться максимально проверенные, стандартизированные и унифицированные архитектурные, программно-алгоритмические, организационно-технологические решения. С другой стороны, с учетом динамики развития ИТ, диалектики средств нападения и развития должны разрабатываться и внедряться новые оригинальные архитектурные, программно-алгоритмические, организационно-технологические решения, обеспечивающие безопасность ИС в новых условиях угроз, с минимизацией затрат и издержек, повышением эффективности и параметров функционирования ИС, снижением требований к пользователям.

# Выводы по вопросу № 1

1. Информационная безопасность  системе национальной безопасности в начале третьего тысячелетия в выходит на первое место.

2. Роль информационной войны сегодня четко осознается российским руководством.

3. Отставание в развитии информационных технологий может привести в перспективе к уязвимости компьютерных сетей страны и в целом всей ее информационной, управленческой инфраструктуры.

4. Информационная безопасность - сравнительно молодая, быстро развивающаяся область информационных технологий, для успешного освоения которой необходимо и важно с самого начала усвоить современный базис, согласованный с другими ветвями информационных технологий.
Успех в области информационной безопасности может принести только системный, комплексный подход.

# 2. Современная постановка задачи обеспечения информационной безопасности

# Проблема обеспечения информационной безопасности

Безопасность как общенаучная категория может быть определена как некоторое состояние рассматриваемой системы, при котором последняя, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних угроз, а с другой – ее функционирование не создает угроз для элементов самой системы и внешней среды.

При таком определении мерой безопасности системы являются:

- с точки зрения способности противостоять дестабилизирующему воздействию внешних и внутренних угроз – степень (уровень) сохранения системой своей структуры, технологии и эффективности функционирования при воздействии дестабилизирующих факторов;
- с точки зрения отсутствия угроз для элементов системы и внешней среды – степень (уровень) возможности (или отсутствия возможности) появления таких дестабилизирующих факторов, которые могут представлять угрозу элементам самой системы или внешней среде.

Интерпретация данных формулировок приводит к следующему определению информационной безопасности.

Информационная безопасность – такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой – ее функционирование не создает информационных угроз для элементов самой системы и внешней среды.

Именно такое понятие информационной безопасности положено в основу Доктрины информационной безопасности (2016 г.) и законодательства в сфере обеспечения информационной безопасности Российской Федерации (дословно – «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 РФ, оборона и безопасность государства».

# Проблема обеспечения информационной безопасности

Информация как непременный компонент любой организованной системы, с одной стороны, легко уязвима (т.е. весьма доступна для дестабилизирующего воздействия большого числа разноплановых угроз), а с другой – сама может быть источником большого числа разноплановых угроз, как для элементов самой системы, так и для внешней среды.

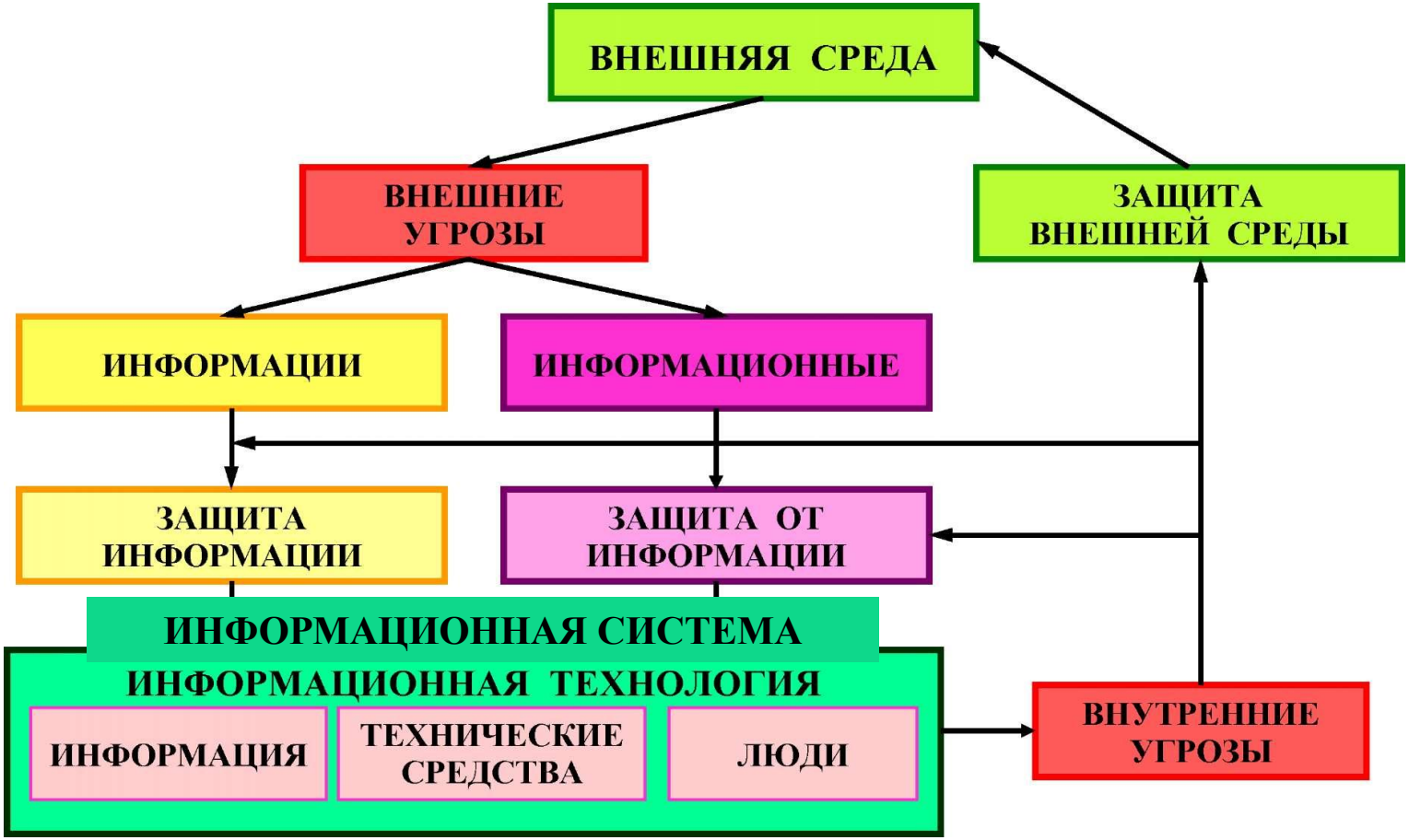
Обеспечение информационной безопасности в общей постановке проблемы может быть достигнуто лишь при взаимоувязанном решении трех составляющих проблем:

1. Защита находящейся в системе информации от дестабилизирующего воздействия внешних и внутренних угроз информации;

2. Защита элементов системы от дестабилизирующего воздействия внешних и внутренних информационных угроз;

3. Защита внешней среды от информационных угроз со стороны рассматриваемой системы.

# Общая схема обеспечения информационной безопасности




**Информационная система** – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т.д.), которые обеспечивают и распространяют информацию (ISO/IEC 2382:2015).

**Информационная система** – это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (ФЗ от 27.07.2006 г. № 149 «Об информации…»).

**Информационная технология** – процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов (ФЗ от 27.07.2006 г. № 149

# Современное состояние изучения и практической разработки проблемы обеспечения информационной безопасности РФ

## I. Проблема защиты информации

1. Проблема получила практически всеобщее признание;
2. Заложены основы разработки теории защиты;
3. Налажено производство средств защиты;
4. Организована планомерная подготовка и повышение квалификации специалистов соответствующего профиля;
5. Создана и совершенствуется государственная система защиты информации;
6. Накоплен значительный опыт практического решения задач защиты информации в системах различного масштаба и функционального назначения.
7. В то же время возрастают масштабы преступности с использованием информационных технологий, рядом зарубежных стран наращиваются возможности информационно-технического воздействия на информационную инфраструктуру в военных целях.

# Современное состояние изучения и практической разработки проблемы обеспечения информационной безопасности

## II. Проблема защиты от информации

Защита от информации заключается в использовании специальных методов и средств в целях предупреждения или нейтрализации негативного воздействия на элементы рассматриваемой системы (людей и технические комплексы) информации, как имеющейся (генерируемой, хранимой, обрабатываемой и используемой) внутри системы, так и поступающей из внешней среды (защита системы от информации).

Так в Доктрине информационной безопасности РФ отмечается, что в настоящее время:

- спецслужбами отдельных государств оказывается информационно-психологическое воздействие, направленное на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящее к подрыву суверенитета и нарушению территориальной целостности других государств;

- существует тенденция к увеличению в зарубежных СМИ объема материалов, содержащих предвзятую оценку государственной политики России; российские СМИ зачастую подвергаются за рубежом откровенной дискриминации, им создаются препятствия для осуществления их профессиональной деятельности;

- наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей...

Информационные угрозы чрезвычайно многообразны, а их воздействие далеко не всегда очевидно. Предотвращение и нейтрализация информационных угроз требуют не столько технических, сколько организационно-правовых и политических решений, причем не только внутригосударственных, но и межгосударственных и даже международных.

## III. Проблема предупреждения негативного воздействия выходной информации системы на элементы внешней среды (информационная экология).

На сегодняшний день в РФ начаты исследования и разработки в области защиты от информации и информационной экологии

# Современная постановка задачи обеспечения информационной безопасности

Традиционно задача обеспечения информационной безопасности представляется как предупреждение несанкционированного получения информации в системах обработки, построенных на базе современных средств электронной вычислительной техники (ЭВТ).

Основное содержание видоизменения постановки задачи обеспечения информационной безопасности может быть сведено к совокупности следующих основных направлений:

1. комплексное **организационное** построение систем защиты информации;
2. комплексное **инструментальное** построение систем защиты информации;
3. организация не только защиты информации, но и защиты от нее;
4. обеспечение условий наиболее эффективного использования информации;
5. переход к так называемой упреждающей стратегии осуществления защитных процессов;
6. расширение рамок защиты от обеспечения компьютерной безопасности до защиты информации на объекте и защиты информационных ресурсов региона и государства;
7. формирование или сохранение «комфортной» информационной среды и достижение «эколого-информационной гармонии».

## Наиболее острые проблемы развития теории и практики обеспечения информационной безопасности

- создание теоретических основ и формирование научно-методологического базиса, позволяющих адекватно описывать процессы в условиях значительной неопределенности и непредсказуемости проявления дестабилизирующих факторов (информационных угроз);
- разработка научно-обоснованных нормативно-методических документов по обеспечению информационной безопасности на базе исследования и классификации угроз информации и выработки стандартов требований к защите;
- стандартизация подходов к созданию систем защиты информации и рационализация схем и структур управления защитой на объектовом, региональном и государственном уровнях.

Решение спектра перечисленных задач имеет важное значение для реализации положений Доктрины информационной безопасности и Стратегии национальной безопасности Российской Федерации.

**Лекция:**
**Концептуальные основы информационной безопасности**

# Доклад закончен. Прошу задать вопросы