“Безопасность есть предотвращение зла”
Платон, определения, стих 415

Методологические подходы к защите информации и принципы ее организации

Вопросы:

1. История развития проблемы защиты информации. Основные положения современной технологии защиты информации
2. Сущность и основные понятия информационной безопасности
3. Виды угроз информационной безопасности РФ
4. Источники угроз информационной безопасности РФ
5. Задачи обеспечения информационной безопасности в различных сферах деятельности
6. Методы обеспечения информационной безопасности РФ в различных сферах
7. Функции и структура государственной системы обеспечения информационной безопасности

1. История развития проблемы защиты информации. Основные положения современной технологии защиты информации

Хронология
процесса развития средств и методов защиты информации
(по эволюции видов носителей информации)

П е р в ы й э т а п
(древность – XIX в)

- связан с появлением возможности фиксации информационных сообщений на твердых носителях, то есть **с изобретением письменности.**

- определяется началом создания осмысленных и самостоятельных средств и методов защиты информации таких как как **шифрование и скрытие.**

Второй этап

(примерно с середины XIX в – 40 г.г. XX в)

- характеризуется появлением **технических средств обработки информации** и возможностью сохранения и передачи сообщений с помощью таких носителей, как электрические сигналы и электромагнитные поля (телефон, телеграф, радио)

- возникли проблемы защиты от так называемых технических каналов утечки (побочных излучений, наводок и др.)

- появились способы шифрования сообщений в реальном масштабе времени (в процессе передачи по телефонным и телеграфным каналам связи) и т. д.

- это период активного развития технических средств разведки, многократно увеличивающих возможности ведения промышленного и государственного шпионажа. Огромные, все возрастающие убытки предприятий и фирм способствовали научно-техническому прогрессу в создании новых и совершенствовании старых средств и методов защиты информации.

Третий этап

(середина XX в.-н.в.)

период массовой информатизации общества

- свя… …автоматизированных систем обработки информ…

Начальный этап
(60-е — начало 70-х гг.)

- внимание к проблеме защиты информации в первую очередь было вызвано все возрастающими финансовыми потерями фирм и государственных орга… …ений в компьютерной сфере

Этап развития
(70-е — начало 80-х гг.)

- выводы западных экспертов показывают, что утечка 20% коммерческой информации в шестидесяти случаях из ста приводит к банкротству фирмы

Современный этап
(с середины 80-х гг. по н.в.)

- все большие финансовые потери… …таки на компьютерные сети. Так, запущенный … …ернет в мае 2000 г. вирус «I love you» вывел из строя свыше 5 млн. компьютеров и нанес ущерб свыше 10 млрд. долларов

Начальный этап
(60-е — начало 70-х гг.)

характеризовался тем, что под защитой информации понималось предупреждение несанкционированного ее получения лицами, не имеющими на то полномочий.

Для этого использовались формальные (то есть функционирующие без участия человека) средства. Наиболее распространенными в автоматизированных системах обработки данных (АСОД) были проверки по паролю прав на доступ к ЭВТ и разграничение доступа к массивам данных. Эти механизмы обеспечивали определенный уровень защиты, однако проблему в целом не решали, поскольку для опытных злоумышленников не составляло большого труда найти пути их преодоления.

Для объектов обработки конфиденциальной информации задачи по ее защите решались в основном с помощью установления так называемого режима секретности, определяющего строгий пропускной режим и жесткие правила ведения секретного документооборота.

Этап развития
(70-е — начало 80-х гг.)

отличается **интенсивными поисками, разработкой и реализацией** способов и средств защиты и определяется следующими характеристиками:

- постепенным осознанием необходимости комплексирования целей защиты

- расширением арсенала используемых средств защиты, причем как по их количеству, так и по их разнообразию. Повсеместное распространение получило комплексное применение технических, программных и организационных средств и методов. Широко стала практиковаться защита информации путем **криптографического ее преобразования**. Стали разрабатываться методы и средства защиты информации на основе **биометрических параметрах человека** (по голосу, почерку, форме руки, отпечаткам пальцев, подписи и т.д.)

- целенаправленным объединением всех применяемых средств защиты в функциональные самостоятельные системы

- нарастание количества средств защиты и принимаемых мер привело в конечном итоге **к проблеме эффективности системы защиты информации**, учитывающей соотношение затраченных на ее создание средств к вероятным потерям от возможной утечки защищаемой информации. Для проведения такой оценки стали применять основные положения теории оценки сложных систем.

- к концу второго периода математически **было доказано**, что обеспечить **полную безопасность информации** в системах ее обработки **невозможно**. Максимально приблизиться к этому уровню можно, лишь решая задачу комплексной защиты информации, опираясь на научно-методологические положения и на хороший инструментарий в виде методов и средств решения соответствующих задач.

Современный этап
(с середины 80-х гг. по н.в.)

характерной особенностью третьего, *современного этапа* комплексной защиты, являются попытки аналитической обработки данных всего имеющегося опыта теоретических исследований и практического решения задач защиты и формирования на этой основе научно-методологического базиса защиты информации.

Основной задачей третьего этапа является перевод процесса защиты информации на строго научную основу.

В настоящее время в России традиционно развивается криптографическое направление защиты информации. Кроме того, свыше 60 вузов занимаются разработкой теоретических подходов к решению проблемы защиты информации, практических методов и средств информационной безопасности, а также подготовкой специалистов по защите информации.

Основные положения современной технологии защиты информации

Технология защиты информации определяется как система знаний и идей, относящихся к защите информации, дающая целостное представление о сущности проблемы защиты, закономерностях ее развития и существенных связях с другими отраслями знания, формирующаяся на основе опыта практического решения задач защиты и определяющая основные ориентиры в направлении совершенствования практики защиты информации.

Составными частями технологии защиты информации являются:

- *полные и систематизированные сведения о происхождении, сущности и содержании проблемы защиты;*
- *систематизированные результаты анализа развития теоретических исследований и разработок, а также опыта практического решения задач защиты;*
- *общие стратегические установки на организацию защиты информации, учитывающие все многообразие потенциальной возможных условий защиты;*
- *методы, средства и способы необходимые для адекватного и наиболее эффективного решения всех задач защиты и содержащие как общеметодологические подходы к решению, так и конкретные прикладные методы решения;*
- *научно обоснованные предложения по организации и обеспечению работ по защите информации;*
- *научно обоснованный прогноз перспективных направлений развития теории и практики защиты информации.*

2. Сущность и основные понятия информационной безопасности

Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.(ФЗ РФ “Об информации, информатизации и защите информации ” от 25.01.95 г.)

Информация (И) как объект защиты имеет следующие особенности и свойства:

- Информация нематериальна;
- Информация доступна человеку, если она содержится на материальном носителе;
- Ценность информации оценивается степенью полезности ее для пользователя;
- Учитывая, что информация может быть для получателя полезной или вредной, что она покупается и продается, то информацию можно рассматривать как товар;
- Ценность информации изменяется во времени;
- Невозможно объективно оценить количество информации;
- При копировании, не изменяющем информационные параметры носителя, количество информации не меняется, а цена снижается.

Классификация информации по режиму доступа

Защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

В соответствии со ст.1 закона РФ “О безопасности”

безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз;

жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

В настоящее время проблема защиты информации рассматривается как проблема информационной безопасности – неотъемлемой составной части национальной безопасности РФ. Это определено в Концепции национальной безопасности РФ и Доктриной информационной безопасности РФ.

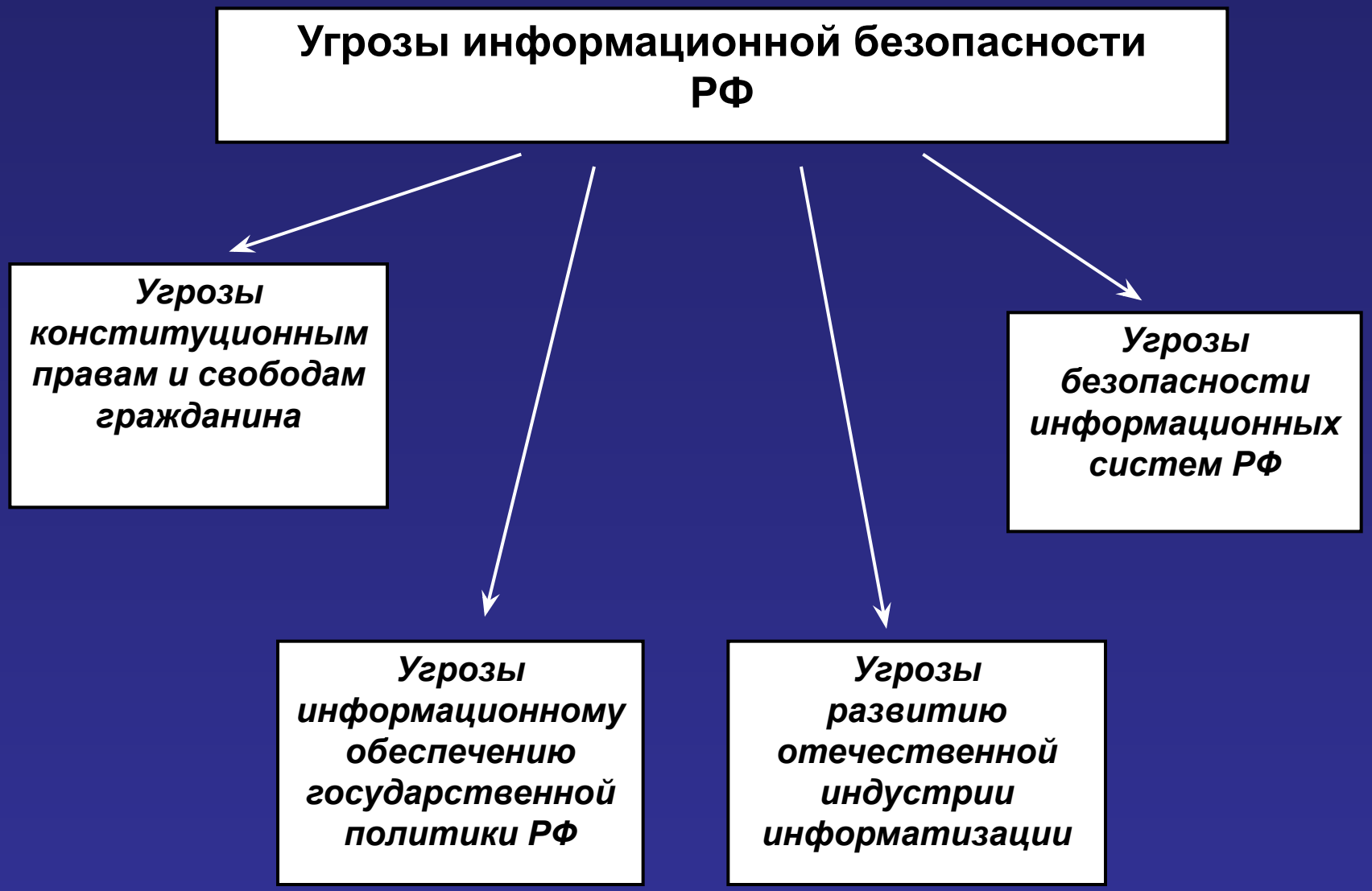
Информационная безопасность РФ определяется как состояние защищенности её национальных интересов в информационной сфере, определяющихся совокупностью интересов личности, общества и государства.

Структура информационной безопасности (И Б)

3. Виды угроз информационной безопасности РФ

Под ***угрозой информационной безопасности*** понимается потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности или секретности информации.

Виды угроз информационной безопасности определены в “Доктрине информационной безопасности Российской Федерации”, утвержденной Президентом РФ 09.09.00. По своей общей направленности угрозы информационной безопасности РФ подразделяются на следующие виды:


Угрозы информационной безопасности РФ
Угрозы конституционным правам и свободам гражданина
Угрозы информационному обеспечению государственной политики РФ
Угрозы развитию отечественной индустрии информатизации
Угрозы безопасности информационных систем РФ

4. Источники угроз информационной безопасности РФ

Источники угроз информационной безопасности РФ подразделяются на внешние и внутренние.

К основным ***внешним источникам*** относятся :

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К наиболее опасным ***внутренним источникам*** относятся :

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

5. Задачи обеспечения информационной безопасности в различных сферах деятельности

К основным мероприятиям можно отнести формирование базы правового обеспечения информационной безопасности нашей страны. Приняты Закон Российской Федерации “О государственной тайне”, Закон Российской Федерации “О коммерческой тайне”, Федеральные законы “Об информации, информатизации и защите информации” и ряд других законов.

Успешному решению вопросов обеспечения ИБ РФ способствуют государственная система защиты информации, система защиты государственной тайны, системы лицензирования деятельности в области защиты государственной тайны и системы сертификации средств защиты информации.

Вместе с тем анализ состояния информационной безопасности Российской Федерации показывает, что ее уровень не в полной мере соответствует потребностям общества и государства.

Причины:

- Современные условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение.

- Противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере существенно затрудняет поддержание необходимого баланса интересов личности, общества и государства в информационной сфере.

- Закрепленные в Конституции Российской Федерации права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки практически не имеют достаточного правового, организационного и технического обеспечения.

- Неудовлетворительно организована защита собираемых федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления данных о физических лицах (персональных данных).

- Нет четкости при проведении государственной политики в области формирования российского информационного пространства, развития системы массовой информации, организации международного информационного обмена и интеграции информационного пространства России в мировое информационное пространство, что создает условия для вытеснения российских информационных агентств, средств массовой информации с внутреннего информационного рынка и деформации структуры международного информационного обмена.

- Недостаточна государственная поддержка деятельности российских информационных агентств по продвижению их продукции на зарубежный информационный рынок.

- Ухудшается ситуация с обеспечением сохранности сведений, составляющих государственную тайну.

- Серьезный урон нанесен кадровому потенциалу научных и производственных коллективов, действующих в области создания средств информатизации, телекоммуникации и связи, в результате массового ухода из этих коллективов наиболее квалифицированных специалистов.

- Отставание отечественных информационных технологий объясняет зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения.

Сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательного решения **важнейших задач**, основными из которых являются:

- разработка основных направлений государственной политики в области обеспечения информационной безопасности Российской Федерации, а также мероприятий и механизмов, связанных с реализацией этой политики;

- развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности Российской Федерации, а также системы противодействия этим угрозам;

- совершенствование нормативной правовой базы обеспечения информационной безопасности Российской Федерации;

- обеспечение технологической независимости Российской Федерации в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность;

- разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами;

- развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;

- обеспечение условий для активного развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем;

- создание единой системы подготовки кадров в области информационной безопасности и информационных технологий.

6. Методы обеспечения информационной безопасности РФ в различных сферах

К правовым методам относят относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации.

Наиболее важными направлениями этой деятельности являются:

- внесение изменений и дополнений в законодательство Российской Федерации, регулирующее отношения в области обеспечения информационной безопасности;
- законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;
- разработка и принятие нормативных правовых актов Российской Федерации, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации;
- создание правовой базы для формирования в Российской Федерации региональных структур обеспечения информационной безопасности.

Основными **организационно-техническими методами** обеспечения информационной безопасности Российской Федерации являются:

- создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;
- усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, в том числе предупреждение и пресечение правонарушений в информационной сфере;
- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации;
- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;
- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;
- формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы обеспечения информационной безопасности Российской Федерации включают:

- разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;

- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

7. Функции и структура государственной системы обеспечения информационной безопасности

Система обеспечения информационной безопасности Российской Федерации предназначена для реализации государственной политики в данной сфере.

Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:

- разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации;
- создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;
- оценка состояния информационной безопасности Российской Федерации, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;
- координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения информационной безопасности Российской Федерации;

- контроль деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, государственных и межведомственных комиссий, участвующих в решении задач обеспечения информационной безопасности Российской Федерации;

- развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств, повышение их конкурентоспособности на внутреннем и внешнем рынке;

- защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и органах государственной власти субъектов Российской Федерации, на предприятиях оборонного комплекса;

- обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;

- совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности Российской Федерации;

- осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются:

- Президент Российской Федерации,
- Совет Федерации Федерального Собрания Российской Федерации,
- Государственная дума Федерального Собрания Российской Федерации,
- Правительство Российской Федерации,
- Совет Безопасности Российской Федерации,
- Федеральные органы исполнительной власти,
- Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации,
- Органы исполнительной власти субъектов Российской Федерации,
- Органы местного самоуправления,
- Органы судебной власти,
- Общественные объединенияb граждане, принимающие в соответствии с законодательством Российской Федерации участие в решении задач обеспечения информационной безопасности Российской Федерации

Конец занятия !

Желаю всем приятного отдыха !