Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан
Ташкентский университет информационных технологий имени Мухаммад ал-Хоразмий

Подготовка кадров в области информационной безопасности и защиты информации в условиях глобализации электросвязи/ИКТ

Профессор Рихси Исаев

Одесса - 2017

Глобальная информатизация и новые информационные технологии открывают возможности во всех сферах человеческой деятельности, порождают новые проблемы, связанные с информационной безопасностью личности, общества и государства. Становится все более очевидным, что и общественный прогресс, и развитие каждого человека сопровождаются и даже в значительной степени определяются развитием их информационной сферы.

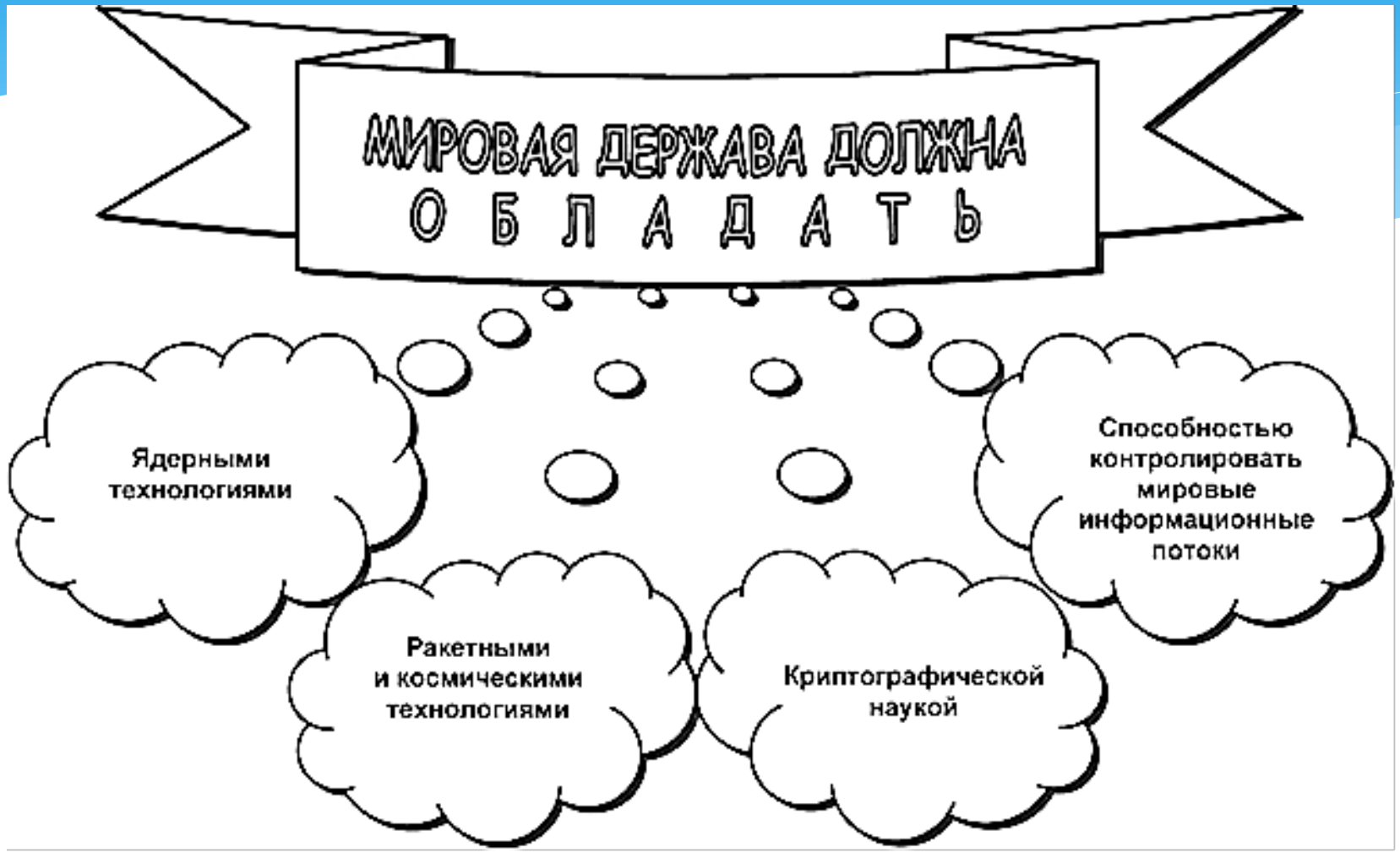
Глобализация, расширяя проблемное поле безопасности, не только изменяет характер традиционных угроз и вызовов, но и порождает новые, складывающиеся в формате нового информационного порядка, основными из которых являются тотальное электронное слежение, манипуляции общественным мнением в глобальном масштабе, использование кибервооружений.

В условиях глобализации информационная безопасность становится ключевым фактором внешнеполитической стратегии государства, выступает одним из политикоформирующих факторов его международной деятельности и устанавливает новые ориентиры его внешнеполитического поведении, трансформируя привычные критерии оценки роли и соотношения военной мощи и политических возможностей в реализации на мировой арене геополитических интересов.

В настоящее время одной из серьёзнейших проблем, активно обсуждаемых в обществе, является информационное противоборство (война). Такая война ведётся с помощью информационного оружия, которое в "умелых руках" становится грозным средством поражения телекоммуникационных и информационных систем. Поражая критически важные объекты телекоммуникационной и информационной инфраструктуры государства, можно резко снизить его обороноспособность и, таким образом, предопределить исход последующей "горячей" войны.

Американский историк криптографии Дэвид Канн ввёл три критерия для определения великой (мировой) державы:

1. Наличие ядерных технологий.
2. Наличие ракетно – космических технологий;
3. Наличие развитой криптографической науки.


МИРОВАЯ ДЕРЖАВА ДОЛЖНА
О Б Л А Д А Т Ь
Ядерными технологиями
Ракетными и космическими технологиями
Криптографической наукой
Способностью контролировать мировые информационные потоки

На современном этапе развития цивилизации весьма четко прослеживается граница между великими державами и остальным миром. И это связано, в первую очередь, с появлением нового критерия в определении великой державы. Этим новым критерием является способность государства обеспечить максимальный контроль мировых информационных потоков.

Объяснение необходимости применения этого критерия вполне очевидно:

- процессы глобализации;
- тотальная информатизация мировой цивилизации и её проникновение во все сферы деятельности государства, общества и человека;
- создание глобальных электронных (сетевых) информационных ресурсов, которые напрямую влияют на эффективность работы всех отраслей экономики и государственной инфраструктуры, внешне - и внутриполитической деятельности, реализации (выполнимость) общегуманитарных и социальных программ (включая образование и медицину), развития научного потенциала и сохранение интеллектуально-культурной массы общества;
- рост международного терроризма, и его попытки расшатывания общемировой стабильности и др.

Контроль мировых информационных потоков (КМИП) — это не просто радиоэлектронная разведка (шпионаж) и добывание информации путем радиоэлектронной разведки (РЭР). Это новое качество (причём принципиально отличное) РЭР. Это отход от традиционных методов ведения РЭР. В основе КМИП лежат сетевые принципы обнаружения и получения информации. Эти принципы предусматривают активные ("наступательные") мероприятия с целью "облегчения/упрощения" доступа к требуемой информации и ресурсам. Для этого необходим специальный доступ к служебной информации, которая, в свою очередь, обеспечивает нормальную работоспособность телекоммуникационных систем и сетей.

Новизна КМИП заключается также и в том, что здесь речь идёт о новой форме информационно-телекоммуникационного пространства, часто называемого "киберпространством". Появление киберпространства наряду с положительными и эффективными факторами воздействия на развитие и гармонизацию мировой цивилизации принесло и новые виды угроз личности, обществу, государству и всему человечеству. Поэтому КМИП:

- с одной стороны, это появление новой формы противоборства (войны), а именно информационного (информационно-технологического);
- а с другой стороны, это форма предупреждения и отражения отрицательных последствий реализации новых "киберугроз".

Фактически КМИП — это контроль киберпространства, который предусматривает новые информационно-телекоммуникационные методы и способы обработки, хранения и доставки данных. Полнота (или максимальность) КМИП предусматривает две составляющих, а именно:

- количественная, то есть какой объём трафика контролируется;
- качественная, насколько точно понимается семантика передаваемого трафика ("осмысление" данных). Другими словами, "какова глубина проникновения" в семантику передаваемой информации (причём, и пользовательской (потребительской), и служебной), чтобы в последующем проводить информационный анализ добытых сообщений для принятия решений по обеспечению национальной безопасности.

Специалисты, занимающиеся проблемой информационной безопасности в Internet, определили несколько видов последствий угроз:

- (несанкционированное) вскрытие;
- обман;
- разрушение;
- захват;
- порча.

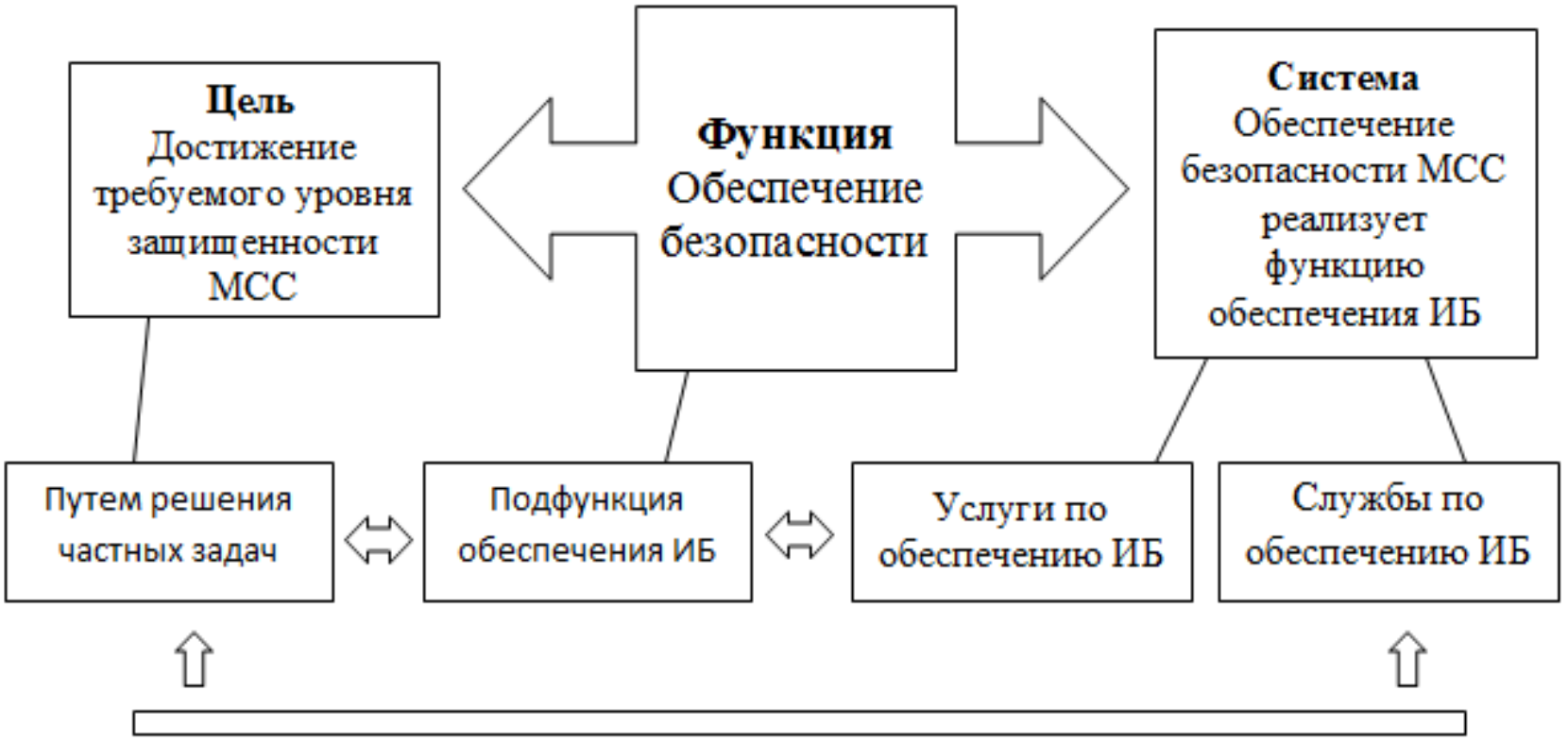
Анализ представленных угроз и последствий их воздействия показывает, что конечными их целями являются:
- информация пользователей, циркулирующая в МСС — чтение и искажение (разрушение) информации и/или нарушение процедур информационного обмена;
- работоспособность самой МСС — чтение и искажение (разрушение) управляющей информации и/или нарушение процедур управления сетевыми (системными) компонентами или всей сетью (системой).

Объекты и реализационные аспекты функции обеспечения ИБ МСС

Под средством обеспечения информационной безопасности понимается комплекс технических устройств (аппаратно-программных, программных и др.), обладающих определенными свойствами и реализующими один или несколько способов защиты информации. При этом несколько различных средств могут реализовать один способ обеспечения информационной безопасности.

Под архитектурой безопасности будем понимать распределение дополнительной(ых) функции(ий) обеспечения безопасности по уровням архитектуры управления МСС с целью обеспечения защиты от угроз ИБ, причем средства каждого уровня обеспечивают защиту только от конкретного вида угроз, к которому наиболее уязвим данный уровень или создание защиты на этом уровне позволяет избежать дублирования функций обеспечения безопасности от этого вида угроз на других уровнях (хотя дублирование таких функций на каждом уровне не исключается).

Средства защиты информации



Задача и состав системы обеспечения безопасности МСС.

В Ташкентском университете информационных технологий имени Мухаммада Ал – Хоразмий открыли факультет информационной безопасности. В этом факультете выпускают бакалавров и магистров по специальности информационной безопасность, информационная безопасность систем и сетей телекоммуникации.

Выпускник должен обладать следующими ключевыми компетенциями:

– способностью проводить мониторинг систем безопасности, применяя межсетевые экраны и системы обнаружения вторжений;

– способностью создавать, внедрять и контролировать исполнение политики безопасности;

– способностью действовать по плану аварийного восстановления данных для операционных систем, баз данных, сетей, серверов и приложений;

– способностью проводить исследования новых продуктов, услуг, протоколов и стандартов для повышения уровня безопасности;

– способностью внедрять новое программное обеспечения и / или технологии;

– способностью проводить регулярные проверки на соответствие использования ресурсов компьютерных систем.

Основными обязательными дисциплинами бакалавров являются:
«Основы информационную безопасность», «Основы криптографии, «Защита программы и данных», «Данные и интеллектуальный анализ» «Безопасность распределенных баз данных», «Безопасность электронной коммерции», «Политика информационной безопасности», «Прикладная криптография».
Получение степени магистра в области информационной безопасности подразумевает теоретическую и практическую подготовку. Студенты осваивают технические и аналитические возможности для защиты данных, файлов, ресурсов компьютера, компьютерной сети, телекоммуникационные систем и сетей а также защиты критически важных национальных электронных инфраструктур. Учебный план программы подготовки создает прочный фундамент в области аудита информационной безопасности и новейшим методам обеспечения защиты информации.

Основными обязательными дисциплинами магистров являются:
«Введение в информационную безопасность», «Информационной безопасность систем сетей телекоммуникации», «Защиты информации оптических систем связи», Защита программы и данных», «Методы криптографических защиты информации».
Выполнение магистерского проекта происходит под руководством преподавателя или группы профессорско-преподавательского состава. Выбор формы реализации проекта и необходимого оборудования остается за преподавателем.

Спасибо за внимание!