РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

по ООП подготовке бакалавров профиля «Безопасность автоматизированных систем» направления 590100 «Информационная безопасность»

Под **результатами обучения** (**РО**) обычно понимаются ожидаемые и измеряемые конкретные достижения студентов и выпускников, выраженные на языке знаний, умений, навыков, способностей, компетенций, и которые описывают, что должен будет в состоянии делать студент/выпускник по завершении всей или части образовательной программы.

РО должны быть простой формулировкой ожидаемых достижений учащегося в процессе обучения. Они

- могут относиться к отдельной курсовой единице или к периоду обучения;
- определяют необходимые условия для присуждения кредитов;
- формулируются профессорско-преподавательским составом.

Первый его вид – РО, которые могут быть проверены в процессе (освоения) программы,

Второй - "Ожидаемые " РО – те, которые предполагаются быть достигнутыми хорошим студентом по завершению программы. (*Этот вид результата не всегда может быть проверен в процессе обучения, но дает возможность работодателям знать ожидаемые стандартные результаты, запланированные программой*).

Полезность и необходимость формулировки РО связано с тем, что

- они помогают обеспечить большую открытость с точки зрения ожиданий,
- проясняют для студента, что следует ожидать от обучения,
- оказывают помощь при разработке качественных, адекватных программ обучения,
- составление учебных планов, разработка проекта и оценка требований напрямую связаны с результатами обучения.

Формулировки РО должны обладать рядом характеристик, из числа которых (в качестве наиболее важных для нас) мы выделяем:

- Конкретность – описание точного состояния, которое студент должен достигнуть в терминах знаний и умений и -
- Привлекательность – обучаемый должен быть заинтересован в достижении сформулированных целей обучения.

Исходя из приведенных соображений и преследуя цели подготовки конкурентно способных на рынке труда бакалавров, мы полагаем, что помимо общих и социально личностных компетенций, указанных в ГОС и ООП подготовки бакалавров профиля «Безопасность автоматизированных систем» направления 590100 «Информационная безопасность» студенты уже с первых двух курсов должны приобретать профессиональные компетенции касательно эксплуатационной деятельности:

I. По результатам обучения за первые два года студенты должны получить, в частности, необходимые

умения по:

- администрированию и эксплуатации защищенных компьютерных систем, их подсистем, средств обеспечения ИБ;
- применению программно-аппаратных, технических средств, методов и правил обеспечения безопасности КС;
- проведению мониторинга эффективности применяемых средств обеспечения ИБ;
- составлению и настройке политики безопасности основных операционных систем, построенных на их основе;
- проведению анализа показателей сетей, применению защищенных протоколов, межсетевых экранов, и средств обнаружений вторжений для ЗИ в сетях;
- осуществлению меры противодействия нарушениям сетевой безопасности с использованием программных и аппаратных средств ЗИ.

Для этого они должны

знать/понимать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- источники угроз ИБ и меры по их предотвращению;
- состав и принципы работы защищенных КС, операционных систем и сред;
- современные программно-аппаратные средства и способы обеспечения ИБ в КС;
- особенности программно-аппаратных и технических средств обеспечения ИБ в операционных системах, компьютерных сетях, базах данных;
- принципы построения современных ОС и особенности их применения для решения задач ЗИ;
- защитные механизмы и средства обеспечения сетевой безопасности, средства, а также методы предотвращения и обнаружения вторжений.

Успешное прохождение производственной практики в конце 3-его года обучения с оформлением соответствующего информационно аналитического отчета может составить основу для последующей работы студентом над ВКР. Поэтому после завершения трехлетнего обучения студенты должны обладать профессиональными компетенциями подавляющей частью касательно эксплуатационной и частично - проектно-технологической и организационно-управленческой деятельности из числа указанных в ГОС и ООП рассматриваемого профиля подготовки. Они будут необходимы им для успешного прохождения производственной практики, привлечения их к участию в решении практических задач организации по разработке и поддержания мер по ЗИ, проведения анализа и оценки состояния ИБ, системы ЗИ или ее компонент, а также составления соответствующих рекомендаций. Для этого они должны быть способны к администрированию и эксплуатации аппаратно-программных средств и систем ЗИ, освоению и применению методов оценивания уровня безопасности АС. Соответственно:

II. После трех лет обучения студенты должны иметь

умения/навыки по**:**

- использованию технической документации, технической литературы и справочников при освоении программно-аппаратных средств ЗИ;

- установке, настройке, эксплуатации и обслуживанию программно-аппаратных средств и систем ЗИ;
- проверке и оценке соответствия реальных характеристик программно-аппаратных средств ЗИ заявленным в технической документации на эти средства;
- проведению анализа показателей сетей и систем связи;
- анализу и оценке угрозы ИБ объекта;
- применению нормативно-правовых актов;
- анализ и оценка работоспособности и эффективности применяемых программно-аппаратных средств ЗИ с целью определения уровня обеспечиваемой ими защищенности и доверия;
- оценке полноты и качества выполнения работниками организации требований политики безопасности;
- составлению аналитического отчета по результатам проведенного анализа и предложений по устранению выявленных уязвимостей;

и **- знать/понимать:**

- требования по составу и характеристикам подсистем ЗИ для различных классов защищенных систем, методы их реализации;
- основные виды управления доступом и информационным потокам в КС, модели и виды политик безопасности КС;
- механизмы реализации вредоносных программно-технических информационных воздействий в КС;
- средства и методы обнаружения и предотвращения вторжений;
- основные методы, системы и средства анализа программных реализаций, технические каналы утечки информации и методы защиты;
- принципы работ и правила эксплуатации известных программно-аппаратных средств ЗИ;
- принципы работ и правила эксплуатации и обслуживанию средств получения, обработки, передачи, отображения и хранения информации**;**
- основные стандарты защищенности КС;
- основные принципы функционирования защищенных распределенных КС;
- порядка оформления технической документации по ЗИ**.**

Обучение студентов на четвертом курсе завершается государственной аттестацией, прохождением пред квалификационной практики, выполнением выпускной квалификационной работы и ее защиты. Для успешного выполнения этой части ООП - проектирования и разработки, модернизации, поддержания и сопровождения (под)систем защиты_информационных объектов/ресурсов, а также анализа и документирования результатов, пред квалификационной практики и оформления ВКР- студенты должны обладать уже компетенциями необходимых для проектно-технологической и организационно-управленческой деятельности:

III. По итогам обучения студенты-бакалавры должны **уметь:**

- разрабатывать требования ТЗ к средствам ЗИ;
- составлять политику безопасности КС с учетом возможных угроз и нарушителей ИБ, действующих нормативных и методических документов;

- проектировать программно-математические и программно-технические средства ЗИ КС;
- выполнять разработку, отладку и тестирование, а также сопровождать разработки средств ЗИ КС

и знать:

- методы и средства ЗИ в компьютерных сетях, операционных системах и СУБД;
- основные виды атак и механизмы их реализации в КС;
- основные формальные модели и политики управления доступом и информационными потоками;
- типовые криптографические протоколы и стандарты;
- методологии и технологии проектирования и разработки программного и аппаратного обеспечения;
- стандарты, постановления, нормативные и методические материалы по вопросам проектирования и обеспечения ИБ КС;
- принципы построения систем ЗИ КС;
- основные принципы функционирования и построения защищенных распределенных КС;
- обще представление о порядке и организации работ по ЗИ.

Подборку профильных дисциплин изучения как для начальных, так и для старших курсов обучения, считаем целесообразным осуществлять в соответствии с выше перечисленными компетенциями. При их составлении были учтены мнения специалистов, работающих в области ЗИ, мнения наших студентов старших курсов и магистров в этой области, привлеченных к обучению наших студентов, а также – компетенции в профессиональном стандарте РФ от 2013 г. для специалиста по информационной безопасности 5, 6 и 7 уровней квалификации.

Зав. каф. ПОКС,
д.ф.-м.н., проф. А.Б.Салиев