



Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

**Аннотации практик образовательной программы высшего образования
по направлению подготовки 10.03.01 Информационная безопасность,
направленность (профиль) «Безопасность автоматизированных систем (по отрасли
или в сфере профессиональной деятельности)»**

УЧЕБНАЯ ПРАКТИКА. ОЗНАКОМИТЕЛЬНАЯ ПРАКТИКА

Практика реализуется кафедрой комплексной защиты информации ФИСБ ИИНТБ РГГУ на базе структурных подразделений РГГУ, предназначенных для практической подготовки или в профильных организациях, расположенных на территории г. Москвы, на основании договора, заключаемого между РГГУ и профильной организацией.

Цель практики: приобретение знаний и умений, необходимых для деятельности, связанной с эксплуатацией и обслуживанием современных средств вычислительной техники, а так же подготовка обучаемых к грамотному и эффективному использованию компьютера как инструмента для решения задач различной степени сложности в области компьютерной безопасности.

Задачи практики:

- изучение основ вычислительной техники;
- изучение принципов работы ЭВМ;
- получение опыта самостоятельной диагностики, ремонта и настройки аппаратных средств вычислительной техники.

В результате прохождения практики обучающийся должен:

Знать:

- понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации
- основные принципы построения компьютера
- принципы и порядок работы информационно-справочных систем; способы поиска и обработки информации, методы работы с научной информацией
- методики проведения теоретических исследований уровней защищенности информационной безопасности объектов и систем
- основные законы и закономерности функционирования экономики; основы экономической теории, необходимые для решения профессиональных и социальных задач
- о эффективности использования стратегии сотрудничества для достижения поставленной цели
- Нормы толерантного восприятия социальных и культурных различий
- Литературные нормы русского языка
- сущность коррупционного поведения и его взаимосвязь с социальными, экономическими, политическими и иными условиями

Уметь:

- составлять и оформлять аналитический отчет по проведенным испытаниям, делать выводы по оценке защищенности на основании аналитического отчета
- обобщать, анализировать и систематизировать научную информацию в области информационной безопасности; пользоваться информационно-справочными системами
- работать с интегрированной средой разработки программного обеспечения
- классифицировать и оценивать угрозы информационной безопасности
- анализировать, толковать и правильно применять правовые нормы о противодействии коррупционному поведению
- применять экономические знания при выполнении практических задач
- понимать цели и задачи безопасности жизнедеятельности, основные понятия, классификацию опасных и вредных факторов среды обитания человека, правовые и организационные основы безопасности жизнедеятельности, обеспечение экологической безопасности
- планировать свое рабочее и свободное время для оптимального сочетания физической и умственной нагрузки и обеспечения работоспособности

Владеть:

- навыками использования профиля защиты и задания по безопасности, формулирования выводов по оценке защищенности
- навыками аргументированного отстаивания собственной позиции по различным философским проблемам
- навыком составления и оформления отчетных документов по результатам обзора научно-технической литературы, нормативных и методических документов
- разработкой алгоритмов решения типовых профессиональных задач
- основными понятиями, связанные с обеспечением информационно-психологической безопасности личности, общества и государства
- навыками работы с законодательными и другими нормативными правовыми актами
- методами выбора инструментальных средств для обработки экономических данных при решении социальных и профессиональных задач

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА. ТЕХНОЛОГИЧЕСКАЯ ПРАКТИКА

Цель практики: закрепить знания и умения по организации и технологии защиты информации, приобретаемые студентами в процессе освоения теоретических курсов и специальных дисциплин. Выработать практические навыки и умения, способствующие комплексному формированию профессиональных компетенций студентов по овладению методами работы с конфиденциальными документами, усвоению организации закрытого делопроизводства в конкретных подразделениях объекта информатизации, приобретению профессиональных навыков и опыта работы в коллективе.

Задачи практики:

- закрепление знаний по разработке организационных мер по обеспечению информационной безопасности на конкретном объекте;
- углубление теоретической подготовки и приобретение практических навыков и компетенций по проведению аналитических исследований по выявлению каналов распространения конфиденциальной информации;
- овладение технологией проведения организационных мероприятий, направленных на предупреждение разглашения/утечки конфиденциальной информации;

- овладение технологией работы с конфиденциальными документами, усвоению организации закрытого делопроизводства в конкретных подразделениях объекта информатизации;
- приобретение практических навыков и компетенций по разработке нормативной и методической документации, регламентирующей организационную защиту информации, работе с конфиденциальными документами и построения защищенного документооборота на предприятии;
- приобретение практических навыков и компетенций по осуществлению профессиональной деятельности в области информационных и коммуникационных технологий (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере).

В результате прохождения практики обучающийся должен

Знать:

- современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности
- современные информационные технологии и программные средства, классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей
- основные нормативные правовые акты, стандарты оформления документации на различных стадиях жизненного цикла информационной системы
- основные нормативные правовые акты, стандарты и документы уполномоченных федеральных органов исполнительной власти по защите информации оформления документации на различных стадиях жизненного цикла информационной системы
- принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
- руководящие документы по защите информации
- назначение и основные технические характеристики информационных систем, их взаимосвязь с техническими средствами охраны и видеонаблюдения; основные руководящие, методические и нормативные документы по организационно-технической защите информации
- типовые решения о необходимости защиты информации, содержащейся в информационной системе
- основных теоретико-методологических положений философии, концептуальных подходов к пониманию природы информации как научной и философской категории
- необходимые для осуществления профессиональной деятельности правовые нормы
- различные приемы и способы социализации личности и социального взаимодействия
- литературную форму государственного языка, основы устной и письменной коммуникации на иностранном языке, функциональные стили родного языка, требования к деловой коммуникации
- основные категории философии, законы исторического развития, основы межкультурной коммуникации
- основные принципы самовоспитания и самообразования, профессионального и личностного развития, исходя из этапов карьерного роста и требований рынка труда

Уметь:

- организовать согласование и утверждение документации по выполняемым работам с учетом требований нормативных документов в области информационной безопасности
- описывать объекты защиты; выявлять источники угроз безопасности ресурсам организации; оценивать возможную величину ущерба от реализации угроз
- разрабатывать политики безопасности
- разрабатывать документы в области обеспечения безопасности информации в АС
- решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
- применять основные нормативные правовые акты, стандарты в области информационной безопасности и защиты информации
- выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности
- выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности

Владеть:

- навыками по разработки аналитического обоснования необходимости создания системы защиты информации в организации с учетом требований нормативных документов в области информационной безопасности
- методикой по разработке технических решений по обеспечению безопасности объекта защиты
- навыками по разработке локальных нормативных документов по защите информации в организации
- практическими навыками по обеспечению защиты информации и организацию работы персонала АС
- навыками по выявлению существенных черт исторических процессов, явлений и событий
- навыками по подготовке обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
- навыками по разработке политики безопасности, составлению документации на различных этапах жизненного цикла информационной системы

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА. ЭКСПЛУАТАЦИОННАЯ ПРАКТИКА

Цель практики – углубление и закрепление теоретических знаний и практических навыков в области подготовки к аттестационным испытания автоматизированной системы и проведению таких испытаний по требованиям безопасности информации.

Задачи практики:

- изучение автоматизированной системы и технологического процесса обработки информации в ней;
- формирование разрешительной системы доступа автоматизированной системы и реализация правил разграничения доступа средствами защиты информации;

- проведение тестирования средств защиты информации автоматизированной системы от несанкционированного доступа на соответствие установленным правилам разграничения доступа;
- исследование уязвимостей и угроз информационной безопасности в автоматизированной.

В результате прохождения практики обучающийся должен

Знать:

- имеющиеся ресурсы и ограничения, оценивает и выбирает оптимальные способы решения поставленных задач
- цели и задачи безопасности жизнедеятельности, основные понятия, классификацию опасных и вредных факторов среды обитания человека, правовые и организационные основы безопасности жизнедеятельности, обеспечение экологической безопасности.
- основные законы и закономерности функционирования экономики;
- основы экономической теории, необходимые для решения профессиональных и социальных задач.
- классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей;
- назначение, функции и обобщённую структуру операционных систем;
- назначение и основные компоненты систем баз данных.
- основы математики, основные понятия теории информации, основные методы оптимального кодирования источников информации
- основополагающие принципы механики, термодинамики, молекулярной физики, квантовой физики; положения электричества и магнетизма, колебаний и оптики

Уметь:

- использования знаний о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения.
- применять экономические знания при выполнении практических задач;
- принимать обоснованные экономические решения в различных областях жизнедеятельности
- применять типовые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети интернет
- исследовать функциональные зависимости, возникающие при решении стандартных прикладных задач
- применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах;
- пользоваться нормативными документами в области технической защиты информации
- строить стандартные процедуры принятия решений, на основе имеющихся экспериментальных данных
- устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учётом требований по обеспечению защиты информации

Владеть:

- методами выбора инструментальных средств для обработки экономических данных при решении социальных и профессиональных задач
- навыками поиска информации в глобальной информационной сети Интернет;
- навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности
- методами расчёта
- принципами формирования политики информационной безопасности объекта информатизации
- навыками по проведению эксперимента по заданной методике с составлением итогового документа
- навыками по осуществлению планирования и организации работы персонала автоматизированной системы с учётом требований по защите информации

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА. ПРЕДДИПЛОМНАЯ ПРАКТИКА

Цель практики – подготовка студента к решению практических задач обеспечения комплексной защиты информации, а также сбор, обработка и систематизация материалов, необходимых для написания выпускной квалификационной работы, т.е. приобретение как персонального практического опыта в исследуемой сфере деятельности, так и приобретение навыков самостоятельной работы по избранному виду профессиональной деятельности

Задачи практики:

- закрепить основные положения теории информационной безопасности и практики защиты информации, основные положения нормативных документов в области комплексной защиты объектов информатизации;
- уметь применять существующие средства защиты информации от несанкционированного доступа;
- овладеть методами синтеза и анализа систем защиты информации, закономерностями построения сложных систем защиты, навыками эксплуатации средств защиты информации, получивших широкое применение в качестве инструментария в современных системах информационной безопасности на предприятии;
- сбор, обработка и систематизация материалов, необходимых для написания выпускной квалификационной работы

В результате прохождения практики обучающийся должен

Знать:

- принципы формирования политики информационной безопасности в информационных системах;
- основные этапы процесса проектирования системы защиты информации и общие требования к содержанию проекта
- нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
- средства, методы и протоколы идентификации, аутентификации и авторизации субъектов в АС
- критерии оценки защищённости автоматизированной системы, основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
- критерии оценки защищённости автоматизированной системы, основные угрозы безопасности информации и модели нарушителя в автоматизированных системах

- правила и порядок разработки концепции средств и систем информатизации в защищённом исполнении,
- правила и порядок разработки технического задания на средство и/или систему информатизации в защищённом исполнении,
- нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
- процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации

Уметь:

- определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите;
- анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации
- разрабатывать документы в области обеспечения безопасности информации в АС при ее эксплуатации (включая управление инцидентами информационной безопасности);
- устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные комплексы с учётом требований по обеспечению защиты информации
- настраивать программное обеспечение системы защиты информации, выявлять и анализировать уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации
- контролировать уровень защищённости информации в автоматизированных системах,
- регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах
- разрабатывать конструкторскую и технологическую документацию на средство и/или систему информатизации в защищённом исполнении на базы данных
- анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации
- разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации

Владеть:

- навыками разработки основных показателей технико-экономического обоснования проектных решений по защите информации
- навыками планирования мероприятий по обеспечению защиты информации и организации работы персонала АС с учётом требований по защите информации
- навыками управления полномочиями пользователей
- навыками планирования и организации работы персонала автоматизированной системы с учётом требований по защите информации
- навыками план проведения аудита защищённости информации в автоматизированных системах
- организационными мерами по защите информации
- навыками разработки аналитического обоснования необходимости создания системы защиты информации в организации

- навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации