МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Чувашский государственный университет имени И.Н. Ульянова»

Факультет информатики и вычислительной техники
Кафедра математического и аппаратного обеспечения информационных систем

«УТВЕРЖДАЮ»
проректор по учебной работе
_____ И.Е. Поверинов
«31» августа 2017 г.

ПРОГРАММА
преддипломной практики
для выполнения выпускной квалификационной работы

Направление	10.03.01 «Информационная безопасность»
Квалификация выпускника	Бакалавр
Профиль	Информационно-аналитические системы финансового мониторинга

Чебоксары - 2017

Рабочая программа основана на требованиях Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность», утвержденного приказом Министерства образования и науки 01.12.2016 г. № 1515, Положения о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования, утвержденного приказом Министерства образования и науки РФ от 27 ноября 2015 г. № 1383.

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):
Доцент, к.ф.-м.н. Д.В.Ильин
старший преподаватель С. О. Иванов

ОБСУЖДЕНО:
на заседании кафедры МиАОИС 30 «августа» 2017 г., протокол № 1

заведующий кафедрой Д. В. Ильин
СОГЛАСОВАНО:

Методическая комиссия факультета ИВТ 30 «августа» 2017 г., протокол № 1

Декан факультета А. В. Щипцова

Директор научной библиотеки П. Д. Никитина

Начальник управления информатизации И. П. Пивоваров

Начальник учебно-методического управления В. И. Маколов

1. Вид, тип практики, формы и способы ее проведения

Преддипломная практика - практика для выполнения выпускной квалификационной работы.

Организация проведения практики осуществляется на основе договоров с организациями, деятельность которых соответствует профессиональным компетенциям, осваиваемым в рамках основной образовательной программы (ООП) (далее – профильная организация). Практика может быть проведена непосредственно в профильных подразделениях Чувашского государственного университета имени И.Н. Ульянова (далее – университет). Рекомендуется проведение преддипломной практики в той же профильной организации, в которой студент-практикант проходил технологическую практику.

Способы проведения практики: выездная и стационарная.

Практика проводится в дискретной форме.

Для руководства практикой, проводимой в профильных подразделениях университета, назначается руководитель практики из числа лиц, относящихся к профессорско-преподавательскому составу кафедры, ответственной за реализацию ООП. Для руководства практикой, проводимой в профильной организации, назначаются руководитель практики из числа лиц относящихся к профессорско-преподавательскому составу кафедры, ответственной за реализацию ООП, и руководитель (руководители) практики из числа работников профильной организации. Направление студента на практику оформляется в виде Путевки студента-практиканта (Приложение 1).

Практика для обучающихся с ограниченными возможностями здоровья и инвалидов проводится с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

2. Цели и задачи обучения при прохождении практики

Практика проводится с целью получения профессиональных умений и опыта профессиональной деятельности, повышения уровня освоения компетенций в профессиональной деятельности, выполнения выпускной квалификационной работы (ВКР).

Во время прохождения практики студент должен получить умения и опыт при решении профессиональных задач, связанных с тематикой ВКР, решать следующие профессиональные задачи

в соответствии с видами профессиональной деятельности:

эксплуатационная деятельность:

установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

администрирование подсистем информационной безопасности объекта;

участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

проектно-технологическая деятельность:

сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

проведение проектных расчетов элементов систем обеспечения информационной безопасности;

участие в разработке технологической и эксплуатационной документации;

проведение предварительного технико-экономического обоснования проектных расчетов;

экспериментально-исследовательская деятельность:

сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

проведение экспериментов по заданной методике, обработка и анализ их результатов;

проведение вычислительных экспериментов с использованием стандартных программных средств;

организационно-управленческая деятельность:

осуществление организационно-правового обеспечения информационной безопасности объекта защиты;

организация работы малых коллективов исполнителей;

участие в совершенствовании системы управления информационной безопасностью;

изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;

контроль эффективности реализации политики информационной безопасности объекта защиты.

Преддипломная практика также решает ряд специфических задач, таких как:

адаптация студента к реальным условиям работы на предприятиях и в организациях;

создание условий для практического применения знаний в области профессиональных, специализированных компьютерных и математических дисциплин;

формирование и совершенствование базовых профессиональных навыков и умений;

диагностика пригодности студента к профессиональной деятельности;

обеспечение успеха дальнейшей профессиональной карьеры.

3. Место практики в структуре образовательной программы

Блок «Практики», вариативная часть.

При прохождении практики используются знания, умения и навыки, сформированные в ходе освоения всех дисциплин и практик, предусмотренных ООП.

Знания, умения и навыки, полученные в результате прохождения практики, используются при прохождения государственной итоговой аттестации.

4. Планируемые результаты обучения при прохождении практики, соотнесенные с результатами освоения образовательной программы

Практика направлена на формирование следующих компетенций:

- способность к самоорганизации и самообразованию (ОК-8);
- способность использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);
- способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (ОПК-6);
- способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);
- способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);
- способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3);
- способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);
- способность принимать участие в организации и сопровождении аттестации

объекта информатизации по требованиям безопасности информации (ПК-5);

– способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6);

– способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7);

– способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);

– способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);

– способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);

– способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11);

– способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);

– способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13);

– способность организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14);

– способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15).

В результате обучения по дисциплине, обучающийся должен (ЗУН):

знать:

– правовые основы профессиональной деятельности;

– основные принципы и приемы самоорганизации и самообразования;

– методы установки и настройки программных, программно-аппаратных и технических средств защиты информации;

– методы и средства проектирования информационно-аналитических систем, подсистем и средств обеспечения информационной безопасности;

– методы организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

– требования к оформлению документов (рабочую и техническую документацию);

уметь:

– использовать в практической деятельности правовые знания;

– планировать и осуществлять свою деятельность с учетом результатов анализа, оценивать и прогнозировать последствия своей профессиональной деятельности;

– применять комплексный подход к обеспечению информационной безопасности объекта защиты;

– проводить обоснование соответствующих проектных решений;

– применять методы организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

– осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности, в том числе в области финансового мониторинга;

– проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

– проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов

– проводить экспериментальные исследования системы защиты информации;

– организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

– оформлять рабочую и техническую документацию;

– организовывать работу малого коллектива исполнителей в профессиональной деятельности;

– организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

владеть навыками:

– использования нормативно-правовых актов в практической деятельности;

– поиска методов решения практических задач на основе информационных технологий, в том числе финансового мониторинга;

– выполнения работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

– использования технологий системного анализа при ведении проектной деятельности;

– оформления документации в области информационной безопасности;

– применения программных средств системного, прикладного и специального назначения, инструментальных средств, языков и систем программирования для решения профессиональных задач;

– администрирования подсистемы информационной безопасности объекта защиты;

– организации и проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

– организации технологического процесса защиты информации ограниченного доступа, в том числе финансовой, в соответствии с нормативными правовыми актами и нормативными методическими документами.

5. Структура и содержание практики

Для освоения программы практики в учебном плане предусмотрено 6 зачетных единиц / 216 академических часов. Продолжительность практики - 4 недели. Практика реализуется в восьмом семестре по окончании сессии. Итоговый контроль: дифференцированный зачет.

5.1. Структура практики

№ п/п	Разделы (этапы) практики	Виды работ на практике, включая самостоятельную работу студентов	Трудоемкость, час	В том числе контактная работа, не менее, час	Формируемые компетенции
1.	Организация практики,	Оформление на практику, прохождение инструктажа	3	0,2	ОК-8, ОПК-6

№ п/п	Разделы (этапы) практики	Виды работ на практике, включая самостоятельную работу студентов	Трудоемкость, час	В том числе контактная работа, не менее, час	Формируемые компетенции
	подготовительный этап	по охране труда, технике безопасности, пожарной безопасности, а также ознакомление с правилами внутреннего трудового распорядка организации, предоставляющей место для прохождения практики			
2.	Производственный этап	Обучение и работа на рабочем месте в качестве стажера-практиканта в соответствии с индивидуальным заданием	195	3,6	ОПК-5 ПК-1- ПК-15
3.	Подготовка отчета	Сбор, обработка и систематизация фактического и литературного материала	15		ОК-8 ПК-1, ПК-7, ПК-8
4.	Защита отчета	Получение отзыва руководителя Публичная защита отчета	3	0,2	ОК-8 ПК-1, ПК-7, ПК-8
	ИТОГО		216	4	
	ИТОГО, з.е.		6		

5.2. Содержание практики

Конкретное содержание практики разрабатывается руководителем практики от кафедры, ответственной за организацию и проведение практики совместно с руководителем практики от профильной организации. Содержание практики отражается в задании на практику студенту-практиканту (Приложение 2).

Выполнение задания должно обеспечивать закрепление, расширение и углубление знаний, умений, навыков в области информационной безопасности, в том числе в области проектирования, эксплуатации информационно-аналитических систем финансового мониторинга. Задание на практику должно предусматривать достижение планируемых результатов обучения при прохождении практики, соотнесенных с результатами освоения образовательной программы.

Задание на практику формулируется с учетом особенностей и характера деятельности профильной организации. В нем должно быть предусмотрено:

– обоснование актуальности темы ВКР, ее теоретической и практической ценности для профильного предприятия или организации;

– проведение всестороннего анализа собранных материалов и данных по теме ВКР, состояния дел с решением проблемы и формулировка основных задач, решаемых в ВКР, формализация требований к программному обеспечению;

– формулировка выводов и обоснование методов, процедур исследования, принимаемых решений по рассматриваемым вариантам и средствам достижения поставленных целей ВКР;

– использование для решения научных и инженерных проблем ВКР современных и перспективных средств разработки программных продуктов, методологий и технологий проектирования программного обеспечения, баз данных и интерфейсов, средств автоматизации разработки, а также технических средств вычислительной, коммуникационной и другой техники с обоснованием их применимости;

– реализацию (полностью или частично) принятых решений.

Рабочий график (план) проведения практики согласуется с руководителем от профильной организации (Приложение 4).

6. Форма отчётности по практике

Формой аттестации практики является зачет с оценкой (дифференцированный зачет). По итогам зачета студенту могут быть выставлены оценки «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно». Для проверки качества прохождения практики, а также полученных знаний, умений и навыков, студенты должны представить руководителю практики от кафедры следующие материалы и документы:

– путевку студента-практиканта, оформленную в соответствии с требованиями и содержащую: отзыв от профильной организации, в которой проходила практика; описание проделанной студентом работы; общую оценку качества его подготовки, умения контактировать с людьми и анализировать ситуацию, умения работать со статистическими данными и т.д.;

– отчет студента-практиканта о проделанной работе во время прохождения практики с указанием полученных новых знаний, умений и навыков (Приложение 3).

Отчёт студента-практиканта по практике должен быть оформлен в соответствии с межгосударственным стандартом ГОСТ 7.32-2001. Отчет студента-практиканта по практике рецензируется и оценивается руководителем практики от кафедры, ответственной за организацию и проведение практики, и руководителем практики от профильной организации. Отчеты защищается перед руководителем практики от кафедры и заведующим кафедрой.

В отчете представляются результаты практики в соответствии с заданием на практику. При написании отчета рекомендуется придерживаться структуры ВКР, которая предусматривает вводную, аналитическую, проектно-конструкторскую и экспериментальную части, выводы, ссылки на литературу и ресурсы сети Интернет. Студенту-практиканту следует иметь в виду, что материалы, представленные в отчете, будут дополняться и дорабатываться в процессе выполнения ВКР. Объем проработки и содержание каждой части отчета обсуждается с руководителями практики.

7. Фонд оценочных средств для проведения аттестации обучающихся по практике

В процессе прохождения практики студентом-практикантом ведется дневник практики, в котором фиксируется вид и продолжительность деятельности в процессе выполнения задания по практике. Дневник является неотъемлемой частью отчета по практике (Приложение 5). Рабочими документами для составления отчета также служат рабочие материалы и документы профильной организации по теме ВКР, разрешенные для изучения и использования студенту-практиканту.

В отчете должна быть представлена следующая информация:

– задание на преддипломную практику соотнесенное с темой ВКР студента-практиканта;

– аннотация к ВКР;

– введение, в котором необходимо кратко обосновать актуальность выбранной темы ВКР, цель разработки темы, объект и предмет исследования, задачи, научную новизну и практическую значимость работы, структуру работы;

– результаты анализа предметной области в рамках темы ВКР (результаты сравнительного анализа существующих программных систем, аналогов разрабатываемой системы, прогнозные характеристики объекта разработки, его показатели качества и эффективности, анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности);

– описание предварительного выбора методологии и технологии проектирования защищенных автоматизированных систем, баз данных и интерфейсов, а также средств разработки, технических средств;

– проектно-конструкторская проработка задач ВКР (проектирование и разработка технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами);

– апробация имеющихся результатов решения задач ВКР (результаты тестирования разработанных мероприятий и отладки систем по обеспечению информационной безопасности, экспериментальное исследование систем защиты информации)

– выводы (достоинства, недостатки, предложения по модернизации и расширению функций, возможностей и интерфейса конкретного программного обеспечения и т.п.);

– список использованной литературы и ресурсов сети Интернет на дату обращения.

Примерные вопросы для оценивания знания теоретического материала в рамках задания на практику:

№	Контрольные вопросы для оценивания знаний	Формируемая компетенция	Критерий оценивания
1.	Как вы планируете и распределяете время во время самостоятельной работы	ОК-8	Полнота ответа, соответствие продемонстрированных при ответах на вопрос знаний материалам отчета о практике. Варианты оценивания: - студент обнаружил всестороннее систематическое знание теоретического материала в рамках задания на практику; - студент твердо знает теоретический материал в рамках задания на практику, грамотно и по существу излагает его, не допускает существенных неточностей в его изложении; - студент имеет знания теоретического материала в рамках задания на практику, но не усвоил его детали, возможно, допускает неточности, недостаточно правильные формулировки при его изложении; - студент демонстрирует незнание теоретического материала в рамках задания на практику
2.	Перечислите ключевые нормативные документы, относящиеся к обеспечению информационной безопасности	ОПК-5	
3.	Назовите источники опасностей и действия по предотвращению инцидентов.	ОПК-6	
4.	Охарактеризуйте особенности установки, настройки и обслуживании программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1	
5.	Охарактеризуйте особенности применения языков, систем и инструментальных средств к выбранной теме выпускной квалификационной работы.	ПК-2	
6.	Охарактеризуйте порядок администрирования подсистемы информационной безопасности объекта защиты	ПК-3	
7.	Назовите принципы и способы реализации политики информационной безопасности	ПК-4	
8.	Охарактеризуйте особенности аттестации объекта информатизации по требованиям безопасности информации	ПК-5	
9.	Охарактеризуйте принципы и подходы, лежащие в основе контроля обеспечения информационной безопасности	ПК-6	
10.	Назовите принципы проектирования и анализа проектных решений системы управления информационной безопасностью	ПК-7	
11.	Какие нормативные и методические документы, относящиеся к обеспечению информационной безопасности, вы применяли на практике	ПК-8, ПК-9	
12.	Охарактеризуйте безопасные технологии работы в интернет	ПК-9	
13.	Охарактеризуйте положения и требования нормативных документов, относящихся к обеспечению информационной безопасности открытых информационных систем	ПК-10	

14.	Какие принципы и подходы вы использовали при экспериментальных исследованиях системы защиты информации	ПК-11, ПК-12	
15.	Охарактеризуйте комплекс мер для обеспечения информационной безопасности в рамках темы ВКР	ПК-13, ПК-14	
16.	Охарактеризуйте особенности организации процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами государственных органов	ПК-14, ПК-15	

Оценивание умения и навыков в рамках задания на практику рекомендуется проводить с учетом следующих дескрипторов компетенций:

№	Дескрипторы компетенций	Формируемая компетенция	Критерий оценивания
	Уметь:		Полнота и соответствие требованиям оформления практического материала в отчете о практике, отзыв профильной организации: Варианты оценивания: - студент в полном объеме представил отчет по практике, оформленный в соответствии с требованиями; имеет положительные отзывы профильной организации; - студент в полном объеме, но с неточностями, представил отчет по практике, оформленный в соответствии с требованиями; имеет в целом удовлетворительные отзывы профильной организации; - студент представил в неполном объеме, с неточностями отчет по практике, оформленный без соблюдений требований; имеет неудовлетворительные отзывы профильной организации
1.	организовывать режим дня при выполнении самостоятельной работы	ОК-8	
2.	использовать в практической деятельности правовые знания;	ОПК-5	
3.	применять приемы оказания первой помощи	ОПК-6	
4.	применять комплексный подход к обеспечению информационной безопасности объекта защиты;	ПК-1, ПК-2, ПК-3, ПК-4	
5.	применять методы организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;	ПК-5	
6.	планировать и осуществлять свою деятельность с учетом результатов анализа, оценивать и прогнозировать последствия своей профессиональной деятельности;	ПК-6, ПК-7	
7.	проводить обоснование соответствующих проектных решений;	ПК-7	
8.	оформлять рабочую техническую документацию;	ПК-8	
9.	осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;	ПК-8, ПК-9	
10.	проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;	ПК-10	
11.	проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	ПК-11	
12.	проводить экспериментальные исследования системы защиты информации;	ПК-12	
13.	организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;	ПК-13	
14.	организовывать работу малого коллектива исполнителей в профессиональной деятельности;	ПК-14	
15.	организовывать технологический процесс	ПК-15	

	защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами государственных органов		
	Владеть навыками:		
1.	расстановки приоритетов и организации рабочего места для эффективного выполнения работ	ОК-8	
2.	поиска, систематизации и применения положений и требований нормативных документов, относящиеся к обеспечению информационной безопасности	ОПК-5, ПК-9	
3.	защиты производственного персонала и населения в условиях чрезвычайных ситуаций	ОПК-6	
4.	выполнения работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;	ПК-1	
5.	использования технологий системного анализа при ведении проектной деятельности;	ПК-4, ПК-7	
6.	оформления документации в области информационной безопасности;	ПК-8	
7.	применения программных средств системного, прикладного и специального назначения, инструментальных средств, языков и систем программирования для решения профессиональных задач;	ПК-2	
8.	администрирования подсистемы информационной безопасности объекта защиты;	ПК-3	
9.	организации и проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;	ПК-5, ПК-6, ПК-10, ПК-11, ПК-12	
10.	организации технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами.	ПК-14, ПК-15	

Критерии оценки:

− оценка «отлично» выставляется студенту, если студент обнаружил всестороннее систематическое знание теоретического материала и практического материала в рамках задания на практику; в полном объеме представил отчет по практике, оформленный в соответствии с требованиями; имеет положительные отзывы руководителя(ей) практики;

− оценка «хорошо» выставляется, если студент твердо знает теоретический материал в рамках задания на практику, грамотно и по существу излагает его, не допускает существенных неточностей в его изложении; в полном объеме представил отчет по практике, оформленный в соответствии с требованиями; имеет положительные отзывы руководителя(ей) практики;

− оценка «удовлетворительно» выставляется студенту, если студент имеет знания только теоретического материала в рамках задания на практику, но не усвоил его детали, возможно, допускает неточности, недостаточно правильные формулировки при его письменном изложении, либо допускает существенные ошибки в изложении теоретического материала; в полном объеме, но с неточностями, представил отчет по практике, оформленный в соответствии с требованиями; имеет в целом удовлетворительные отзывы руководителя(ей) практики;

− оценка «неудовлетворительно» выставляется студенту, если студент без уважительных причин допускал пропуски в период прохождения практики; допускал принципиальные ошибки в выполнении заданий по практике, либо не выполнил задание; представил в неполном объеме, с неточностями отчет по практике, оформленный без соблюдений требований; имеет неудовлетворительные отзывы руководителя(ей) практики.

8. Перечень учебной литературы и ресурсов сети «Интернет», необходимых для проведения практики

Электронный каталог и электронные информационные ресурсы, предоставляемые научной библиотекой ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://library.chuvsu.ru/

8.1. Рекомендуемая основная литература

№ п/п	Наименование
1.	Грекул В.И. Проектирование информационных систем. Курс лекций [Электронный ресурс] : учебное пособие для студентов вузов, обучающихся по специальностям в области информационных технологий / В.И. Грекул, Г.Н. Денищенко, Н.Л. Коровкина. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 303 c. — 978-5-4487-0089-7. — Режим доступа: http://www.iprbookshop.ru/67376.html
2.	Липаев В.В. Сопровождение и управление конфигурацией сложных программных средств [Электронный ресурс] / В.В. Липаев. — Электрон. текстовые данные. — М. : СИНТЕГ, 2006. — 348 c. — 5-89638-095-X. — Режим доступа: http://www.iprbookshop.ru/27300.html
3.	Петренко С.А. Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться. Информационные технологии для инженеров [Электронный ресурс] / С.А. Петренко, А.В. Беляев. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 400 c. — 978-5-4488-0122-8. — Режим доступа: http://www.iprbookshop.ru/63959.html
4.	Анализ состояния защиты данных в информационных системах [Электронный ресурс] : учебно-методическое пособие / В.В. Денисов. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2012. — 52 c. — 978-5-7782-1969-4. — Режим доступа: http://www.iprbookshop.ru/44897.html
5.	Паршин К.А. Оценка уровня информационной безопасности на объекте информатизации [Электронный ресурс] : учебное пособие / К.А. Паршин. — Электрон. текстовые данные. — М. : Учебно-методический центр по образованию на железнодорожном транспорте, 2015. — 96 c. — 978-5-89035-821-9. — Режим доступа: http://www.iprbookshop.ru/45291.html
6.	Моделирование систем и процессов. Практикум : учебное пособие для академического бакалавриата / В. Н. Волкова [и др.] ; под ред. В. Н. Волковой. — М. : Издательство Юрайт, 2017. — 295 с. [Электронный ресурс]. URL: https://www.biblio-online.ru/book/3DF77B78-AF0B-48EE-9781-D60364281651
7.	Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс] : учебное пособие / Ю.Н. Сычев. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 195 c. — 978-5-4487-0128-3. — Режим доступа: http://www.iprbookshop.ru/72345.html
8.	Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс] : учебное пособие / Г.П. Жигулин. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2014. — 174 c. http://www.iprbookshop.ru/67451.html
9.	Гатчин Ю.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / Ю.А. Гатчин, Е.В. Климова. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2009. — 84 c. http://www.iprbookshop.ru/67463.html

8.2. Рекомендуемая дополнительная литература

№ п/п	Наименование
1.	Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. - М.: ООО "Издательство Машиностроение", 2009. - 508 с. URL: http://window.edu.ru/resource/611/63611
2.	Титов А.А. Технические средства защиты информации [Электронный ресурс] : учебное пособие / А.А. Титов. — Электрон. текстовые данные. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. — 194 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/13989.html
3.	Анализ состояния защиты данных в информационных системах [Электронный ресурс] : учебно-

	методическое пособие / В.В. Денисов. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2012. — 52 c. — 978-5-7782-1969-4. — Режим доступа: http://www.iprbookshop.ru/44897.html
4.	Анализ состояния защиты данных в информационных системах [Электронный ресурс] : учебно-методическое пособие / В.В. Денисов. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2012. — 52 c. — 978-5-7782-1969-4. — Режим доступа: http://www.iprbookshop.ru/44897.html
5.	Демидов А.А. Проблемы контроля безопасности информации на объектах телекоммуникационных систем органов государственного управления [Электронный ресурс] : учебное пособие / А.А. Демидов. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2015. — 70 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/67555.html
6.	Паршин К.А. Оценка уровня информационной безопасности на объекте информатизации [Электронный ресурс] : учебное пособие / К.А. Паршин. — Электрон. текстовые данные. — М. : Учебно-методический центр по образованию на железнодорожном транспорте, 2015. — 96 c. — 978-5-89035-821-9. — Режим доступа: http://www.iprbookshop.ru/45291.html
7.	Тони Хаулет Защитные средства с открытыми исходными текстами. Практическое руководство по защитным приложениям [Электронный ресурс] : учебное пособие / Хаулет Тони. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 608 c. — 978-5-4487-0065-1. — Режим доступа: http://www.iprbookshop.ru/67392.html
8.	Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" [Электронный ресурс]: http://ivo.garant.ru/#/document/12148555/paragraph/3471:3

8.3. Правовые нормативные акты и нормативно-методические документы (доступны на кафедре)

1. Руководящий документ. Защита информации. Комплектующие помехоподавляющие изделия электронной техники, радиоэкранирующие и радиопоглощающие материалы. Общие технические требования. Утвержден приказом Гостехкомиссии России от 31.08.2001 № 355.
2. Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи. Утвержден приказом ФСТЭК России от 15.03.2012 № 27.
3. Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 02.03.2001 № 282.
4. Требования к межсетевым экранам. Утверждены приказом ФСТЭК России от 09.02.2016 № 9.
5. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 06.12.2011 № 638.
6. Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20.03.2012 № 28. Требования к средствам доверенной загрузки. Утверждены приказом ФСТЭК России от 27.09.2013 № 119. Требования к средствам контроля съемных машинных носителей информации. Утверждены приказом ФСТЭК России от 28.07.2014 № 87.
7. Требованиям безопасности информации к операционным системам, утвержденным приказом ФСТЭК России от 19.08.2016 г. № 119.
8. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 15.02.2008.
9. Временная методика оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.

10. Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.

11. Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.

12. Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.

9. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем

Программное обеспечение, профессиональные базы данных, информационно-справочные системы, предоставляемые управлением информатизации ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://ui.chuvsu.ru/*

9.1. Программное обеспечение

№ п/п	Наименование	Условия доступа/скачивания
1.	MS Office/ LibreOffice	из внутренней сети университета (договор)
2.	MS Windows/Arch linux	
3.	Visual Studio Community	http://www.visualstudio.com/ru/vs/community
4.	SPID_AlgorithmPoC-0-4-6	https://sourceforge.net/projects/spid/files/
5.	Snort2_9_11_1	https://www.snort.org/
6.	Wireshark 2.6.3	https://www.wireshark.org/
7.	Zabbix	https://www.zabbix.com/download
8.	Clonezilla	https://clonezilla.org/downloads.php
9.	rsync	https://rsync.samba.org/
10.	AVG AntiVirus Free	https://www.avg.com/ru-ru/homepage#pc
11.	Avast Free Antivirus	http://avast-anti-virus.ru/?yclid=5762528100398929218
12.	Kaspersky Free	https://www.kaspersky.ru/free-antivirus
13.	360 Total Security	https://www.360totalsecurity.com/ru/
14.	Pycharm	https://www.jetbrains.com/pycharm/
15.	Strawberry Prolog	http://www.dobrev.com/
16.	Octave	https://www.gnu.org/software/octave/
17.	Oracle VirtualBox	https://www.virtualbox.org/

9.2. Базы данных, информационно-справочные системы

№ п/п	Наименование программного обеспечения	Условия доступа/скачивания
1.	Гарант	из внутренней сети университета (договор)
2.	Консультант +	
3.	База данных угроз безопасности информации	https://bdu.fstec.ru/

9.3. Рекомендуемые интернет-ресурсы и открытые онлайн курсы

№ п/п	Наименование интернет ресурса	Режим доступа
1.	ISO 27000 Международные стандарты управления информационной безопасностью.	http://iso27000.ru
2.	Информационная безопасность. Практика информационной безопасности.	http://dorlov.blogspot.com
3.	SecurityLab. Информационный портал по безопасности.	http://www.securitylab.ru
4.	Российская Государственная Библиотека	http://www.rsl.ru

5.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
6.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
7.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
8.	Научная электронная библиотека	http://elibrary.ru
9.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
10.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru
11.	Техническая защита информации ФСТЭК	http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty
12.	Центр по лицензированию, сертификации и защите государственной тайны ФСБ	http://clsz.fsb.ru/

10. Описание материально-технической базы, необходимой для проведения практики

В соответствии с договорами на проведение практики между университетом и профильной организацией, студенты могут пользоваться ресурсами подразделений (бюро, отделов, лабораторий и т.п.) библиотекой, технической и другой документацией профильной организации и университета необходимыми для успешного освоения студентами программы практики и выполнения ими индивидуальных заданий на практику.

Учебные аудитории для самостоятельных занятий оснащены автоматизированным рабочим местом (АРМ) преподавателя (лаборанта и(или) техника) и пользовательскими АРМ по числу обучающихся, объединенных локальной сетью («компьютерный» класс), с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде университета.

Приложение 1. Путевка студенту-практиканту

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Чувашский государственный университет имени И.Н. Ульянова»
(ФГБОУ ВО «ЧГУ им. И.Н. Ульянова»)

ПУТЕВКА
студента-практиканта

Студент____курса_____факультета

_____
(фамилия

_____
имя, отчество)

согласно договору № _____ от _____

командируется _____

для прохождения производственной (_____)

практики по направлению подготовки/специальности

_____

с «___» _____20___ г. по «___» _____ 20___ г.

Зав.кафедрой _____(_____)
расшифровка подписи

Специалист
по учебно-методической работе_____ (_____)
М.П. расшифровка подписи

Практикант явился на работу _____ 20 г.
Назначен в распоряжение (кого)_____

_____
_____
_____
_____

Заполняется Предприятием

М.П. «_____» _____20 г.

Продолжение Приложения 1

Общий отзыв администрации предприятия
о работе практиканта
(по окончании практики)

_____

_____

_____

_____

_____

_____

_____

Студент пробыл на практике _____ мес.

Размер оплаты (помесячно)_____

_____

Дата откомандирования с места практики «____» _____20__г.

М.П. **Подписи**

Время предоставления отчета на кафедру

_____

Отзыв руководителя практики от кафедры об отчете

_____

_____

_____

_____

Руководитель практики _____(_____)
расшифровка подписи

«____» _____20___г.

Приложение 2. Пример задания на практику студенту-практиканту

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Чувашский государственный университет имени И.Н. Ульянова»
(ФГБОУ ВО «ЧГУ им. И.Н. Ульянова»)
Факультет информатики и вычислительной техники
Кафедра математического и аппаратного обеспечения информационных систем

ЗАДАНИЕ
студенту-практиканту

_____
ФИО студента-практиканта, группа

для преддипломной практики для выполнения выпускной квалификационной работы на (в)

_____
наименование профильной организации/подразделения университета

1. Ведение и оформление дневника практики.
2. Прохождение инструктажа по охране труда, технике безопасности, пожарной безопасности, а также ознакомление с правилами внутреннего трудового распорядка организации, предоставляющей место для прохождения практики.
3. Ознакомление с базой практики, системой защиты информации, в том числе финансовой, выпускаемой продукцией, структурой исследовательских, проектно-конструкторских и иных подразделений, их ролью, задачами и взаимосвязями с другими подразделениями;
4. Ознакомление с научной организацией труда в исследовательских, проектно-конструкторских и иных подразделениях профильной организации;
5. Исходные данные для выполнения ВКР по теме: _____
_____
_____
_____
_____
6. Рекомендованная литература и ресурсы сети Интернет для выполнения ВКР:
_____
_____
_____
7. Выполнение индивидуального задания:

– обоснование актуальности темы ВКР, ее теоретической и практической ценности для профильного предприятия или организации;

– проведение всестороннего анализа собранных материалов и данных по теме ВКР, состояния дел с решением проблемы и формулировка основных задач, решаемых в ВКР, формализация требований к программному обеспечению;

– формулировка выводов и обоснование методов, процедур исследования, принимаемых решений по рассматриваемым вариантам и средствам достижения поставленных целей ВКР;

– использование для решения научных и инженерных проблем ВКР современных и перспективных средств разработки программных продуктов, методологий и технологий проектирования программного обеспечения, баз данных и интерфейсов, средств

автоматизации разработки, а также технических средств вычислительной, коммуникационной и другой техники с обоснованием их применимости;

- реализация (полностью или частично) принятых решений.

8. Планируемый результат:

_____
_____
_____
_____
_____

Руководитель практики от кафедры _____/_____

Дата выдачи задания «____»_____20__ г.

Согласовано:
Руководитель практики от профильной организации (при наличии)
_____/_____

Дата согласования «____»_____20__ г

Приложение 3. Отчет по практике. Титульный лист

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Чувашский государственный университет имени И.Н. Ульянова»
(ФГБОУ ВО «ЧГУ им. И.Н. Ульянова»)

Факультет информатики и вычислительной техники
Кафедра математического и аппаратного обеспечения информационных систем

ОТЧЕТ О ПРЕДДИПЛОМНОЙ ПРАКТИКЕ
ДЛЯ ВЫПОЛНЕНИЯ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

на базе _____
(наименование профильной организации/ структурного подразделения университета)

Студент-практикант 4 курса
направления подготовки
«Информационная
безопасность», группа
_____ _____ _____
подпись, дата ФИО

Руководитель, _____ кафедры
должность
математического и аппаратного
обеспечения информационных
систем_____ _____ _____
уч. степень, уч. звание подпись, дата ФИО

Руководитель от профильной
организации (при наличии),
_____ _____ _____
должность подпись, дата
ФИО

Заведующий кафедрой
математического и аппаратного
обеспечения информационных
систем, _____ _____ _____
уч. степень, уч. звание подпись, дата ФИО

Чебоксары 201_

Продолжение Приложения 3. Отчет по практике. Лист содержания

РЕФЕРАТ

Отчет _____ с., _____ табл., _____ рис. , ____ прил.

5-15 КЛЮЧЕВЫХ СЛОВ

Предметом практики является

Цель практики …..

В ходе практики …..

По результатам практики …..

СОДЕРЖАНИЕ

Приложение 4. Рабочий график (план) проведения практики

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Чувашский государственный университет имени И.Н. Ульянова»
(ФГБОУ ВО «ЧГУ им. И.Н. Ульянова»)
Факультет информатики и вычислительной техники
Кафедра математического и аппаратного обеспечения информационных систем

РАБОЧИЙ ГРАФИК (ПЛАН)
ПРОВЕДЕНИЯ ПРЕДДИПЛОМНОЙ ПРАКТИКИ
ДЛЯ ВЫПОЛНЕНИЯ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

на базе _____
(наименование профильной организации/ структурного подразделения университета)

_____
(ФИО студента-практиканта, группа)
10.03.01 «Информационная безопасность»
(профиль «Информационно-аналитические системы финансового мониторинга»)
(направление/специальность подготовки, профиль/специализация)

№ п/п	Разделы (этапы) практики	Виды работ на практике, включая самостоятельную работу студентов	Трудоемкость, час	Дата, интервал дат
1.	Организация практики, подготовительный этап	Оформление на практику, прохождение инструктажа по охране труда, технике безопасности, пожарной безопасности, а также ознакомление с правилами внутреннего трудового распорядка организации, предоставляющей место для прохождения практики	3	
2.	Производственный этап	Обучение и работа на рабочем месте в качестве стажера-практиканта в соответствии с индивидуальным заданием	195	
3.	Подготовка отчета	Сбор, обработка и систематизация фактического и литературного материала	15	
4.	Защита отчета	Получение отзыва руководителя Публичная защита отчета	3	
	ИТОГО		216	

Руководитель практики от кафедры _____/_____

Дата выдачи графика «____»_____20__ г.

Согласовано:
Руководитель практики от профильной организации (при наличии)
_____/_____

Дата согласования «____»_____20__ г

Приложение 5. Дневник прохождения практики

ДНЕВНИК
ПРОХОЖДЕНИЯ ПРЕДДИПЛОМНОЙ ПРАКТИКИ
ДЛЯ ВЫПОЛНЕНИЯ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

на базе _____
(наименование профильной организации/ структурного подразделения университета)

_____
(ФИО студента-практиканта, группа)

10.03.01 «Информационная безопасность»
(профиль «Информационно-аналитические системы финансового мониторинга»)
(направление/специальность подготовки, профиль/специализация)

№ п/п	Разделы (этапы) практики	Виды работ на практике, включая самостоятельную работу студентов	Трудоемкость, час	Дата, интервал дат
1.	Организация практики, подготовительный этап	Оформление на практику, прохождение инструктажа по охране труда, технике безопасности, пожарной безопасности, а также ознакомление с правилами внутреннего трудового распорядка организации, предоставляющей место для прохождения практики	3	
2.	Производственный этап	Обучение и работа на рабочем месте в качестве стажера-практиканта в соответствии с индивидуальным заданием:	195	
			6	
		...	9	
			…	
			9	
3	Подготовка отчета	Сбор, обработка и систематизация фактического и литературного материала	15	
432	Защита отчета	Получение отзыва на рабочем месте Публичная защита отчета	3	
	ИТОГО		216	

Студент практикант _____/_____

Руководитель практики от профильной организации _____/_____

Дата составления «____»_____20__ г.

Изменения и (или) дополнения от 01.09.2018 г (протокол №1 МК факультета ИВТ) к программе **преддипломной практики для выполнения выпускной квалификационной работы** (10.03.01 Информационная безопасность, направление «Информационно-аналитические системы финансового мониторинга»):

к перечню учебной литературы и ресурсов сети «Интернет»

№ п/п	Рекомендуемая основная литература
1.	Грекул В.И. Проектирование информационных систем. Курс лекций [Электронный ресурс] : учебное пособиендля студентов вузов, обучающихся по специальностям в области информационных технологий / В.И. Грекул, Г.Н. Денищенко, Н.Л. Коровкина. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 303 c. — 978-5-4487-0089-7. — Режим доступа: http://www.iprbookshop.ru/67376.html
2.	Липаев В.В. Сопровождение и управление конфигурацией сложных программных средств [Электронный ресурс] / В.В. Липаев. — Электрон. текстовые данные. — М. : СИНТЕГ, 2006. — 348 c. — 5-89638-095-X. — Режим доступа: http://www.iprbookshop.ru/27300.html
3.	Петренко С.А. Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться. Информационные технологии для инженеров [Электронный ресурс] / С.А. Петренко, А.В. Беляев. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 400 c. — 978-5-4488-0122-8. — Режим доступа: http://www.iprbookshop.ru/63959.html
4.	Анализ состояния защиты данных в информационных системах [Электронный ресурс] : учебно-методическое пособие / В.В. Денисов. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2012. — 52 c. — 978-5-7782-1969-4. — Режим доступа: http://www.iprbookshop.ru/44897.html
5.	Аккредитация и аттестация [Электронный ресурс] : сборник нормативных актов и документов / . — Электрон. текстовые данные. — Саратов: Ай Пи Эр Медиа, 2015. — 77 c. — 978-5-905916-68-7. — Режим доступа: http://www.iprbookshop.ru/30281.html
6.	Моделирование систем и процессов. Практикум : учебное пособие для академического бакалавриата / В. Н. Волкова [и др.] ; под ред. В. Н. Волковой. — М. : Издательство Юрайт, 2017. — 295 с. [Электронный ресурс]. URL: https://www.biblio-online.ru/book/3DF77B78-AF0B-48EE-9781-D60364281651
7.	Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс] : учебное пособие / Ю.Н. Сычев. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 195 c. — 978-5-4487-0128-3. — Режим доступа: http://www.iprbookshop.ru/72345.html
8.	Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс] : учебное пособие / Г.П. Жигулин. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2014. — 174 c. http://www.iprbookshop.ru/67451.html
9.	Гатчин Ю.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / Ю.А. Гатчин, Е.В. Климова. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2009. — 84 c. http://www.iprbookshop.ru/67463.html
	Рекомендуемая дополнительная литература
1.	Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. - М.: ООО "Издательство Машиностроение", 2009. - 508 с. URL: http://window.edu.ru/resource/611/63611
2.	Титов А.А. Технические средства защиты информации [Электронный ресурс] : учебное пособие / А.А. Титов. — Электрон. текстовые данные. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. — 194 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/13989.html
3.	Анализ состояния защиты данных в информационных системах [Электронный ресурс] : учебно-методическое пособие / В.В. Денисов. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2012. — 52 c. — 978-5-7782-1969-4. — Режим доступа: http://www.iprbookshop.ru/44897.html
4.	Семенов Ю.А. Процедуры, диагностики и безопасность в Интернет [Электронный ресурс] / Ю.А. Семенов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 581 c. — 978-5-94774-708-9. — Режим доступа: http://www.iprbookshop.ru/62827.html
5.	Демидов А.А. Проблемы контроля безопасности информации на объектах телекоммуникационных систем органов государственного управления [Электронный ресурс] : учебное пособие / А.А.

	Демидов. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2015. — 70 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/67555.html
6.	Пелешенко В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления [Электронный ресурс] : учебное пособие / В.С. Пелешенко, С.В. Говорова, М.А. Лапина. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2017. — 86 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/69405.html
7.	Тони Хаулет Защитные средства с открытыми исходными текстами. Практическое руководство по защитным приложениям [Электронный ресурс] : учебное пособие / Хаулет Тони. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 608 c. — 978-5-4487-0065-1. — Режим доступа: http://www.iprbookshop.ru/67392.html
	Рекомендуемые интернет-ресурсы и открытые онлайн курсы
1.	ISO 27000 Международные стандарты управления информационной безопасностью. URL:http://iso27000.ru
2.	Информационная безопасность. Практика информационной безопасности. URL:http://dorlov.blogspot.com
3.	SecurityLab. Информационный портал по безопасности. URL:http://www.securitylab.ru
4.	Российская Государственная Библиотека. URL:http://www.rsl.ru
5.	Государственная публичная научно-техническая библиотека России. URL:http://www.gpntb.ru
6.	Фундаментальная библиотека Нижегородского государственного университета. URL:http://www.unn.ru/library
7.	Научная библиотека Казанского государственного университета. URL:http://lsl.ksu.ru
8.	Научная электронная библиотека. URL:http://elibrary.ru
9.	Полнотекстовая библиотека учебных и учебно-методических материалов. URL:http://window.edu.ru
10.	Электронно-библиотечная система IPRbooks. URL:http://www.iprbookshop.ru
11.	Техническая защита информации ФСТЭК. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty
12.	Центр по лицензированию, сертификации и защите государственной тайны ФСБ. URL: http://clsz.fsb.ru/
	Нормативные методические документы в области информационной безопасности ограниченного доступа
1.	Руководящий документ. Защита информации. Комплектующие помехоподавляющие изделия электронной техники, радиоэкранирующие и радиопоглощающие материалы. Общие технические требования. Утвержден приказом Гостехкомиссии России от 31.08.2001 № 355.
2.	Временная методика оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.
3.	Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи. Утвержден приказом ФСТЭК России от 15.03.2012 № 27.
4.	Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.
5.	Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.
6.	Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.
7.	Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 02.03.2001 № 282.
8.	Требования к межсетевым экранам. Утверждены приказом ФСТЭК России от 09.02.2016 № 9.
9.	Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 06.12.2011 № 638.
10.	Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20.03.2012 № 28. Требования к средствам доверенной загрузки. Утверждены приказом ФСТЭК России от 27.09.2013 № 119. Требования к средствам контроля съемных машинных носителей информации. Утверждены приказом ФСТЭК России от 28.07.2014 № 87.

11.	Требованиям безопасности информации к операционным системам, утвержденным приказом ФСТЭК России от 19.08.2016 г. № 119.
12.	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 15.02.2008.

Декан факультета  А.В. Щипцова