МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»	«УТВЕРЖДАЮ»
Руководитель ОП	Заведующий кафедрой информационной безопасности
_____ Варлатая С.К.	_____ Добржинский Ю.В.
«05» июля 2018 г	«05» июля 2018 г.

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Преддипломная практика

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль подготовки: «Комплексная защита объектов информатизации»

Квалификация (степень) выпускника: бакалавр

Владивосток
2018

1. НОРМАТИВНАЯ ДОКУМЕНТАЦИЯ, РЕГЛАМЕНТИРУЮЩАЯ ПРОЦЕСС ОРГАНИЗАЦИИ И ПРОХОЖДЕНИЯ ПРАКТИКИ

Программа разработана в соответствии с требованиями:

- образовательного стандарта, самостоятельно установленного ДВФУ по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом ректора ДВФУ от 20.07.2017 №12-13-1479;

- положения о практике обучающихся, осваивающих образовательные программы высшего образования – программы бакалавриата, программы специалитета и программы магистратуры в школах ДВФУ, утвержденного приказом ректора ДВФУ от 14.05.2018 № 12-13-870.

2. ЦЕЛИ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Целями преддипломной практики являются:

– закрепление теоретических знаний по блоку профессиональных дисциплин;

– развитие и накопление специальных умений и навыков, изучение организационно-методических и нормативных документов и участие в их разработке для решения отдельных задач по месту прохождения практики;

– формирование и развитие общекультурных и профессиональных компетенций;

– ознакомление с содержанием основных работ и исследований, выполняемых на предприятии или в организации по месту прохождения практики;

– изучение особенностей строения, состояния, поведения и/или функционирования служб защиты информации предприятий;

– усвоение приемов, методов и способов обработки, представления и интерпретации результатов исследований, проведенных в ходе практики;

– приобретение практических навыков по разработке и использованию информационных технологий обработки данных;

– развитие элементов профессиональной квалификации, связанных с использованием информационных технологий;

– изучение действующих на предприятии информационных систем;

– приобретение практических навыков в будущей профессиональной деятельности.

3. ЗАДАЧИ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Задачами производственной преддипломной практики являются:

– поиск и изучение информации из различных источников (учебная и научная литература, периодические издания, материалы конференций, ресурсы сети Интернет) о предметной области, о существующих методах и подходах к решению функциональных задач данной предметной области, об аналогах и прототипах;

– изучение существующей информационной системы предприятия или организации;

– всесторонний анализ собранной информации с целью дальнейшего выбора оптимальных и обоснованных проектных решений;

– полное освоение теоретического материала, необходимого для решения практических задач в предметной области;

– полное выполнение цикла проектирования, завершающееся получением решений, пригодных для непосредственной реализации при дальнейшем выполнении выпускной квалификационной работы.

4. МЕСТО ПРЕДДИПЛОМНОЙ ПРАКТИКИ В СТРУКТУРЕ ОП

Производственная преддипломная практика входит в Блок 2 «Практики» образовательной программы бакалавриата. Преддипломная практика проводится концентрированно на 4 курсе в 8 семестре.

5. ТИПЫ, СПОСОБЫ, МЕСТО И ВРЕМЯ ПРОВЕДЕНИЯ УЧЕБНОЙ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Преддипломная практика, как правило, проводится на предприятиях производственного профиля или на выпускающей кафедре информационной безопасности ШЕН ДВФУ. Практика проводится концентрированно в четвертом семестре. Продолжительность практики – 4 недели.

Способы проведения практики:

- стационарная;

- выездная.

Преддипломная практика – практическая часть образовательного процесса подготовки обучающихся, проходящая организациях различных отраслей, сфер и форм собственности, в академических и ведомственных научно-исследовательских организациях, органах государственной и муниципальной власти, деятельность которых соответствует направлению подготовки (профильные организации), учреждениях системы высшего и среднего профессионального образования, системы дополнительного образования, в структурных подразделениях университета по направлению подготовки под руководством руководителей практики.

Перед началом практики проводится организационное собрание, на котором студентам сообщается вся необходимая информация по проведению преддипломной практики.

Руководство практикой возлагается на руководителя практики, совместно с которым студент составляет программу прохождения практики В ней планируется вся работа практиканта:

– изучение специальной литературы и документации;

– изучение структуры организации и управления деятельностью подразделения, где проводится практика;

– принципы формирования комплекса мер по обеспечению информационной безопасности предприятия;

– составление отчёта по преддипломной практике.

6. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ПРОХОЖДЕНИЯ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

В результате прохождения данной производственной преддипломной практики у обучающихся формируются следующие профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
ПК-1 способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знает	методику проведения обследования организации и выявления информационных потребностей пользователей
	Умеет	выявлять информационные потребности пользователей, формировать требования к информационной системе
	Владеет	методикой обследования организации и выявления информационных потребностей пользователей
ПК-2 способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знает	способен разрабатывать, внедрять и адаптировать прикладное программное обеспечение
	Умеет	основные среды для разработки программного обеспечения.
	Владеет	внедрять и адаптировать прикладное программное обеспечение.
ПК-3 способность администрировать подсистемы информационной безопасности объекта защиты	Знает	основные этапы разработки информационных систем и нормативную сопроводительную документацию.
	Умеет	разрабатывать сопроводительную документацию
	Владеет	нормативными требованиями ГОСТ и ИСО МЭК по разработке и сопровождению процессов создания информационных систем по стадиям жизненного цикла.
ПК-4 способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Знает	принципы и методы организационной защиты информации
	Умеет	анализировать и оценивать степень риска проявления факторов опасности систем «Человек – среда обитания», осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности
	Владеет	методами анализа и формализации

		информационных процессов объекта и связей между ними
ПК-5 способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Знает	тактико-технические характеристики основных телекоммуникационных систем, сигналов и протоколов, применяемых для передачи различных видов сообщений
	Умеет	отслеживать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи
	Владеет	навыками анализа основных электрических характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений; анализа сетевых протоколов
ПК-6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Знает	методы сбора первичной информации
	Умеет	проводить экспертизу собранной информации
	Владеет	навыками формализации требований пользователей заказчика
ПК-7 способность разрабатывать программы и методики испытаний программных, программно-аппаратных и технических средств и систем обеспечения информационной безопасности	Знает	методы и программно-аппаратные средства защиты программного обеспечения от несанкционированного изучения, копирования и модификации
	Умеет	настраивать каналы безопасного обмена информацией в локальных и распределен-ных автоматизированных системах
	Владеет	программно-аппаратными комплексами управления ключами, сертификатами и правами пользователей в защищенных автоматизированных системах
ПК-8 способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Знает	основы информационной безопасности
	Умеет	принимать участие в эксплуатации подсистем управления информационной безопасностью
	Владеет	навыками применения мер по защите информации
ПК-9 способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Знает	подсистемы информационной безопасности объекта
	Умеет	администрировать подсистемы информационной безопасности объекта
	Владеет	навыками администрирования

ПК-10 способность оценивать уязвимости информационных систем, разрабатывать требования и критерии оценки информационной безопасности, согласованных со стратегией развития информационных систем	Знает	структуру баз данных с конфиденциальной информацией
	Умеет	защищать конфиденциальную информацию.
	Владеет	навыками использования средств программно-аппаратной и инженерно-технической защиты информации.
ПК-11 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	Знает	модульную структуру подсистемы безопасных современных операционных систем и способы интеграции средств защиты
	Умеет	настраивать системы обнаружения вторжений и антивирусные системы
	Владеет	программно-аппаратными комплексами управления ключами, сертификатами и правами пользователей в защищенных автоматизированных системах
ПК-12 способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Знает	организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации
	Умеет	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации
	Владеет	методами формирования требований по защите информации
ПК-13 способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Знает	методы и алгоритмы управления и генерации ключей и их аппаратно-программная реализация и применение в автоматизированных системах
	Умеет	настраивать системы предотвращения вторжений
	Владеет	инструментарием, обеспечивающим программно-аппаратную защиту информационных ресурсов от изучения, модификации и копирований
ПК-14 способность принимать участие в проведении экспериментальных исследований системы защиты информации	Знает	принципы организации информационных систем в соответствии с требованиями по защите информации
	Умеет	анализировать и оценивать угрозы информационной безопасности объекта
	Владеет	методами анализа и формализации

		информационных процессов объекта и связей между ними
ПК-15 способность разрабатывать планы и программы проведения научных исследований и технических разработок	Знает	место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России
	Умеет	анализировать и оценивать угрозы информационной безопасности объекта
	Владеет	профессиональной терминологией в области информационной безопасности
ПК-16 способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Знает	правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны
	Умеет	анализировать и оценивать угрозы информационной безопасности объекта
	Владеет	методами формирования требований по защите информации
ПК-17 способность организовывать работу малого коллектива исполнителей в профессиональной деятельности	Знает	методы и принципы организационной защиты информации на предприятии
	Умеет	формулировать и настраивать политику безопасности распространенных систем, а также локальных вычислительных сетей, построенных на их основе
	Владеет	методами формирования требований по защите информации на предприятии
ПК-18 способность организовывать и выполнять работы по созданию, монтажу, наладке, испытанию и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности	Знает	основные факты о системах с открытым ключом
	Умеет	строить и изучать математические модели криптоалгоритмов
	Владеет	основным криптографическим инструментарием, необходимым для построение защищенных информационных систем
ПК-19 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	Знает	первоочередные мероприятия по обеспечению безопасности информации АС организации
	Умеет	пользоваться нормативными документами по защите информации
	Владеет	методиками проверки защищенности объектов информации на соответствие требований нормативных документов

ПСК-3.1 способность проводить совместный анализ функционального процесса объекта защиты и применяемых информационных технологий и технических средств с целью определения возможных источников информационных угроз, их вероятных целей и тактики	Знает	возможные источники информационных угроз
	Умеет	определять вероятные цели и тактики источников информационных угроз
	Владеет	способностью проводить совместный анализ функционального процесса объекта защиты и применяемых информационных технологий и технических средств
ПСК-3.2 способность формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта и его информационных составляющих, с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объектов и локализации защищаемых элементов	Знает	деструктивные воздействия на информационные ресурсы
	Умеет	формировать предложения по тактике защиты объектов и локализации защищаемых элементов
	Владеет	способностью формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта
ПСК-3.3 способность разрабатывать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, проводить выбор необходимых технологий и технических средств, организовать внедрение и последующее сопровождение	Знает	комплекс организационных и технических мер по обеспечению информационной безопасности
	Умеет	проводить выбор необходимых технологий и технических средств, организовать внедрение и последующее сопровождение
	Владеет	способностью разрабатывать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации

7. СТРУКТУРА И СОДЕРЖАНИЕ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Общая трудоемкость преддипломной практики составляет 4 недели / 6 зачетных единиц, 216 часов

№ п/п	Разделы (этапы) практики	Виды учебной работы на практике, включая самостоятельную работу студентов и трудоемкость	Формы текущего контроля

		(в часах)				
		Ознакомительные лекции	Самостоятельная работа	Практическое участие	Обсуждение с руководителем	
1	Подготовительный	8	-	-	-	ПР-1
2	Основной	-	48	60	40	УО-2, ПР-9
3	Итоговый	-	20	20	20	УО-2, отчёт о практике

8. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ НА ПРЕДДИПЛОМНОЙ ПРАКТИКЕ

Учебно-методическое обеспечение самостоятельной работы студентов на производственной преддипломной практике направлено на создание условий выполнения индивидуальных заданий по практике. Учебно-методическое обеспечение должно обеспечивать выполнение индивидуальных заданий. Учебно-методическое обеспечение должно располагать методическими материалами для студентов, раскрывающими организацию практики, выполнение индивидуальных заданий, оценивание результатов прохождения практики в компетентностном формате и включает:

- положение о порядке проведения практики студентов;
- методические указания студентам по прохождению практики;
- индивидуальное задание и календарный план проведения практики;
- методические рекомендации по контролю и оцениванию практики;

- график консультаций.

В процессе производственной преддипломной практики студентами изучаются и отражаются в отчете по практике нижеследующие основные группы вопросов о деятельности органа государственной или муниципальной власти, предприятия, или организации:

1. Правила внутреннего распорядка, охраны труда, противопожарной защиты предприятия (организации), содержание уставных, нормативно-правовых документов, отражающих требования по информационной безопасности.

2. Документы, характеризующие организационную структуру предприятия (организации), кадровое, правовое и информационное обеспечение его (ее) деятельности, состав и функции, выполняемые каждым подразделением учреждения.

3. Перечень и содержание организационных документов для службы делопроизводства и электронного документооборота, основные принципы и правила работы с документами ограниченного доступа.

4. Перечень и содержание документов по организации охраны и режима.

5. Перечень и содержание документов по организации работы с персоналом в области информационной безопасности.

6. Перечень и основное содержание организационных документов, обеспечивающих защиту информации на предприятии (политика информационной безопасности, модель угроз информационной безопасности, положение по обработке и защите персональных данных).

7. Рекомендации по совершенствованию системы защиты информации документооборота предприятия (организации), с учетом применения криптографических средств защиты информации.

8. Рекомендации по совершенствованию административного уровня информационной безопасности предприятия (организации), с учетом

внедрения, или доработки организационных документов по обеспечению информационной безопасности.

9. Рекомендации по внедрению многорубежной модели обеспечения физической защиты объекта информатизации и автоматизированной системы (один из отдельных объектов).

10. Классифицированную модель угроз информационной безопасности для объекта информатизации и автоматизированной системы (один из отдельных объектов).

11. Перечень мероприятий по работе с персоналом организации (предприятия) для обеспечения защиты информации и при эксплуатации автоматизированной системы.

12. Структурно-функциональную модель, отражающая топологию локальной (распределенной) сети предприятия (организации), с учетом внедрения средств программно-технической, криптографической и физической защиты информации.

9. ФОРМЫ АТТЕСТАЦИИ (ПО ИТОГАМ ПРАКТИКИ)

Учебная преддипломная практика считается завершенной при условии выполнения студентами всех требований программы практики.

Аттестации по итогам практики проводится в виде собеседования и оценивается в форме зачёта с оценкой.

Студенты оцениваются по итогам всех видов деятельности при наличии документации по практике.

Студент должен предоставить по итогам практики:

1) дневник преддипломной практики;

2) отчет по преддипломной практике;

3) отзыв предприятия.

В дневнике должны быть отражены результаты текущей работы и выполненные задания. Дневник преддипломной практики заполняется лично студентом. Записи о выполненных работах производятся по мере

необходимости, но не реже раза в один – два дня. Достоверность записей проверяется руководителем и заверяется его подписью.

Индивидуальное задание на ознакомительную практику студента должно иметь отметку о выполнении запланированной работы. Отчет по практике должен иметь описание проделанной работы; самооценку о прохождении практики; выводы и предложения по организации практики и подпись студента.

Текст отчета должен быть отредактирован и напечатан с соблюдением правил оформления, предусмотренных требованиями к оформлению письменных работ, выполняемых студентами и слушателями ДВФУ.

Отзыв предприятия должен включать оценку прохождения практики студентом и также включать рекомендации по оптимизации процесса организации практики.

10. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕПРОИЗВОДСТВЕННОЙ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Основная литература

1. Аверченков В.И., Рытов М.Ю., Кувыклин А.В., Гайнулин Т.Р. Разработка системы технической защиты информации [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.].— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 187 с.— Режим доступа: http://www.iprbookshop.ru/7005.html

2. А. В. Иванов, В. А. Трушин Защита речевой информации от утечки по акустоэлектрическим каналам Новосибирск Изд-во НГТУ 2012, - 43 с. http://lib.dvfu.ru:8080/lib/item?id=IPRbooks:IPRbooks-44919&theme=FEFU

3. М. Ф. Шкляр. Основы научных исследований : учебное пособие Москва : Дашков и К°, 2013. 243 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:673741&theme=FEFU

Дополнительная литература

1. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации: учебное пособие - Санкт-Петербург: СПб: НИУ ИТМО, 2011, 2011. - 112 с. http://lib.dvfu.ru:8080/lib/item?id=IPRbooks:IPRbooks-65808&theme=FEFU

2. Б. И. Герасимов, В. В. Дробышева, Н. В. Злобина Основы научных исследований : учебное пособие Москва : Форум, : [Инфра-М], 2013. 269 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:752201&theme=FEFU

3. Медведев Н.В. Дипломное проектирование по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем» [Электронный ресурс]: методические указания/ Медведев Н.В., Квасов П.М.— Электрон. текстовые данные.— М.: Московский государственный технический университет имени Н.Э. Баумана, 2011.— 80 с.— Режим доступа: http://www.iprbookshop.ru/30962.html

Перечень информационных технологий и программного обеспечения

№ п/п	Место расположения компьютерной техники, на которой установлено программное обеспечение, количество рабочих мест	Перечень программного обеспечения
1.	Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16

		лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020. 7) Dallas Lock. Поставщик Конфидент. Партнерское соглашение БП-8-16/576-16-ЦЗ/1 от 23.11.2016. Срок действия договора 23.11.2019. Лицензия до 23.11.2019.
2.	Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 314, Аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.
3.	Аудитория для самостоятельной работы аспирантов: Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус А , ауд. А1017.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно.

		5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОИЗВОДСТВЕННОЙ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Материально-техническое обеспечение производственной преддипломной практики обеспечивается вузом, ДВФУ.

Производственная преддипломная практика проводится на базе кафедры информационной безопасности, в лабораториях и компьютерных аудиториях школы естественных наук, оснащенных компьютерами классами и мультимедийными (презентационными) системами, с подключением к общекорпоративной компьютерной сети ДВФУ и сети Интернет. При прохождении практики используется библиотечный фонд научной библиотеки ДВФУ, электронные библиотечные системы (ЭБС), заключившие договор с ДВФУ.

При прохождении производственной преддипломной практики на предприятиях используется программное и техническое обеспечение базовых производственных предприятий и организаций.

№ п/п	Наименование оборудованных помещений и помещений для самостоятельной работы с указанием адреса	Перечень основного оборудования
1.	Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Моноблок HPP-B0G08ES#ACB/8200E AIO i52400S 500G 4.0G 28 PC Электронная доска Poly Vision Walk-and-Talk WTL 1810 Мультимедийная аудитория: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47", Full HD, LG M4716 CCBA Мультимедийный проектор Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800

		Сетевая видеокамера Multipix MP-HD718
2.	Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 314, Аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Компьютер DNS Office (автоматизированное рабочее место), Рабочее место сотрудников в составе: системный блок, клавиатура, мышь, монитор 17" Aser-173 Мультимедийное оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47", Full HD, LG M4716 CCBA Мультимедийный проектор Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718
3.	Аудитория для самостоятельной работы аспирантов: Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус А , ауд. А1017.	"Читальные залы Научной библиотеки ДВФУ с открытым доступом к фонду: Моноблок Lenovo C360G-i34164G500UDK – 15 шт. Интегрированный сенсорный дисплей Polymedia FlipBox - 1 шт. Копир-принтер-цветной сканер в e-mail с 4 лотками Xerox WorkCentre 5330 (WC5330C – 1 шт. Скорость доступа в Интернет 500 Мбит/сек. Рабочие места для людей с ограниченными возможностями здоровья оснащены дисплеями и принтерами Брайля; оборудованы: портативными устройствами для чтения плоскопечатных текстов, сканирующими и читающими машинами видеоувеличителем с возможностью регуляции цветовых спектров; увеличивающими электронными лупами и ультразвуковыми маркировщиками"

Составитель: доцент кафедры информационной безопасности Варлатая С.К., кандидат технических наук, доцент _____

Программа практики обсуждена на заседании кафедры информационной безопасности, протокол от «05» июля 2018 г. №13.