

АННОТАЦИЯ рабочей программы «Учебная практика (учебно-лабораторная)» для студентов 1,2,3 курса очной формы обучения по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Вид практики	Учебная
Тип практики	Учебно-лабораторная
Способ проведения практики	Стационарная
Форма проведения практики	Непрерывная
Цель практики	Цель практики – ознакомление студентов с распределенными системами управления версиями на примере GIT, системой верстки LaTeX и использование этих систем для создания презентации о выполненном задании одного из списка задач с сайта cryptohack.org в системе компьютерной алгебры Sage.
Компетенции, формируемые в результате освоения практики	<p>ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;</p> <p>ОПК-7 Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ.</p>
Результаты освоения образовательной программы (ИДК)	<p>ОПК-2.1. Понимает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности.</p> <p>ОПК-2.2. Выбирает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности.</p> <p>ОПК-2.3. Обладает навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности.</p> <p>ОПК-7.1. Разрабатывает программы на языках высокого и низкого уровня.</p> <p>ОПК-7.2. Применяет известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач.</p> <p>ОПК-7.3. Осуществляет обоснованный выбор инструментария</p>

		программирования и способов организации программ.
Знания, умения и навыки, получаемые в процессе прохождения практики	и	<p>В результате прохождения практики обучающийся должен:</p> <p>Знать: основы систем управления версиями GIT, синтаксис GIT команд, синтаксис основных команд верстки LaTeX; базовый синтаксис языка Python (Sage) для решения криптоаналитической задачи по курсу типа CTF.</p> <p>Уметь: работать с системой управления версиями на примере GitHub/GitLab, оформлять презентации в пакете Beamer от LaTeX; моделировать криптоаналитическую задачу формата CTF на языке Python.</p> <p>Владеть: навыками использования систем управления версиями Git, навыками верстки в LaTeX и создания презентаций с помощью пакета Beamer; навыками решения задач формата CTF на языке Python.</p>
Структура содержания практики	и	<p>Подготовительный этап:</p> <ol style="list-style-type: none"> 1. Организационное собрание для разъяснения целей, задач, содержания и порядка прохождения практики. 2. Обязательный инструктаж по охране труда, инструктаж по технике безопасности, пожарной безопасности. 3. Инструктаж по установке Git, LaTeX и TexStudio. 4. Выбор задания типа CTF с сайта cryptihack.org <p>Производственный этап:</p> <p>Выполнение выбранного задания с сайта cryptihack.org задания на языке Python/Sage</p> <p>Заключительный этап:</p> <ol style="list-style-type: none"> 1. Подготовка презентации. 2. Представление результатов в виде презентации и демонстрации работы программы. 3. Защита отчёта по практике
Разработчики		Киришанова Е.А., PhD, доцент ИФМН и ИТ БФУ им. И.Канта,

АННОТАЦИЯ рабочей программы «Производственная практика (проектно-технологическая)» для студентов 4,5 курса очной формы обучения по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Вид практики	Производственная практика
Тип практики	Проектно-технологическая
Способ проведения практики	Стационарная
Форма проведения практики	Непрерывная
Цель практики	<p>Целью практики является получение студентами профессиональных умений и опыта профессиональной деятельности.</p> <p>Задачами практики являются:</p> <ol style="list-style-type: none"> 1) развитие способностей студента к самостоятельной аналитической работе; 2) развитие навыков студента к применению знаний и умений, полученных в результате теоретической подготовки, к выполнению практических заданий в области обеспечения компьютерной безопасности, управления информационной безопасностью, эксплуатации технических и программно-аппаратных средств защиты информации; 3) развитие умения анализировать существующие системы компьютерной (информационной) безопасности на предмет стойкости, эффективности и соответствия нормативным документам; 4) развитие навыков эскизного и технического проектирования систем (подсистем, элементов) обеспечения компьютерной (информационной) безопасности, систем управления информационной безопасностью, планирования работы систем эксплуатации технических и программно-аппаратных средств защиты информации; 5) формирование и развитие у студентов устойчивого интереса к профессиональной деятельности, потребности в самообразовании.
Компетенции, формируемые в результате освоения практики	<p style="text-align: center;">УК – 6</p> <p>Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни</p> <p style="text-align: center;">ОПК – 1</p> <p>Способен оценивать роль информации, информационных</p>

	<p>технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства</p> <p style="text-align: center;">ОПК-4</p> <p>Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности;</p> <p style="text-align: center;">ОПК-5</p> <p>Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;</p> <p style="text-align: center;">ОПК-6</p> <p>Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;</p> <p style="text-align: center;">ОПК-11</p> <p>Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации</p> <p style="text-align: center;">ОПК – 14</p> <p>Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации;</p> <p style="text-align: center;">ОПК-15</p> <p>Способен администрировать компьютерные сети и контролировать корректность их функционирования</p> <p style="text-align: center;">ОПК-16</p> <p>Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.</p>
<p>Результаты освоения образовательной программы (ИДК)</p>	<p>УК.6.1. Определяет свои личные ресурсы, возможности и ограничения для достижения поставленной цели;</p> <p>УК.6.2. Создает и достраивает индивидуальную траекторию саморазвития при получении основного и дополнительного образования;</p> <p>УК.6.3. Умеет обобщать и транслировать свои индивидуальные достижения на пути реализации задач саморазвития; умеет рационально распределять временные и информационные ресурсы;</p>

ОПК.1.1. Демонстрирует знания понятия информации, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики;

ОПК.1.2. Демонстрирует знание основных средств и способов обеспечения информационной безопасности, принципов построения систем защиты информации;

ОПК.1.3. Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности; классифицирует и оценивает угрозы информационной безопасности для объекта информатизации;

ОПК-4.1. Демонстрирует знание физических законов и моделей, необходимых при решении задач обеспечения защиты информации;

ОПК-4.2. Применяет необходимые физические законы и модели для решения обеспечения защиты информации;

ОПК-4.3. Владеет навыками моделирования для решения задач обеспечения защиты информации;

ОПК-5.1. Демонстрирует знание нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в организации; классифицирует и оценивает угрозы информационной безопасности для объекта информатизации;

ОПК-5.2. Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации;

ОПК-5.3. Анализирует и разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации;

ОПК-6.1. Понимает угрозы безопасности информации и возможные пути их реализации, нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ОПК-6.2. Способен организовать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ОПК-6.3. Обладает навыками организации защиты информации

ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ОПК-11.1. Знает меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты;

ОПК-11.2. Способен формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности;

ОПК-11.3. Владеет навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты;

ОПК-14.1. Знает методы, алгоритмы и инструменты для проектирования баз данных, администрирования систем управления базами данных в соответствии с требованиями по защите информации;

ОПК-14.2. Умеет проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации;

ОПК-14.3. Владеет навыками проектирования баз данных, администрирования систем управления базами данных в соответствии с требованиями по защите информации;

ОПК-15.1. Знает устройство, порядок администрирования и контроля функционирования компьютерных сетей;

ОПК-15.2. Умеет осуществлять администрирование и контроль корректности функционирования компьютерных сетей;

ОПК-15.3. Владеет навыками администрирования и контроля функционирования компьютерных сетей;

ОПК-16.1. Знает устройство, принципы функционирования, порядок настройки, мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях;

ОПК-16.2. Умеет осуществлять мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;

ОПК-16.3. Владеет навыками мониторинга работоспособности и анализа эффективности средств защиты информации в

	компьютерных системах и сетях.
Знания, умения и навыки, получаемые в процессе прохождения практики	<p>В результате прохождения производственной практики (научно-исследовательская работа) обучающийся должен:</p> <p style="text-align: center;">знать:</p> <ul style="list-style-type: none"> - необходимые математические методы для решения задач обеспечения защиты информации; - методику разработки программ на языках высокого и низкого уровня; - методы защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации; - меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты; - современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности; - принципы и способы администрирования операционных систем, методы и алгоритмы восстановления работоспособности прикладного и системного программного обеспечения; - принципы функционирования программных и программно-аппаратных средств защиты информации в компьютерных системах, принципы и методы разработки их компонент, методики анализа их безопасности; - устройство, принципы функционирования, порядок настройки, мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях <p style="text-align: center;">уметь:</p> <ul style="list-style-type: none"> - применять совокупность необходимых математических методов для решения задач обеспечения защиты информации; - применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач; - осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов; - решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации; - формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по

	<p>обеспечению информационной безопасности;</p> <p style="text-align: center;">владеть:</p> <ul style="list-style-type: none"> - разработкой, обоснованием и реализацией на практике процедур решения задач обеспечения защиты информации; - обоснованным выбором инструментария программирования и способов организации навыками решения профессиональных задач с широким использованием актуальной научно-технической литературы; - навыками решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации; - навыками мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях; - навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.
<p>Структура и содержание практики</p>	<p style="text-align: center;">Организационный этап:</p> <ol style="list-style-type: none"> 1. Определение базы прохождения практики. 2. Организационное собрание для разъяснения целей, задач, содержания и порядка прохождения практики. 3. Обязательный инструктаж по охране труда (вводный и на рабочем месте), инструктаж по технике безопасности, пожарной безопасности. 4. Ознакомление с правилами внутреннего распорядка на базе прохождения практики. 5. Получение и согласование индивидуального задания по прохождению практики. 6. Разработка и утверждение индивидуальной программы практики и графика выполнения исследования. 7. Получение документации по практике (программы практики, индивидуального задания на практику, плана-графика прохождения практики и дневника практики с направлением на практику) в сроки, определенные программой. 8. Изучение правовых основ, базовых нормативных и локальных правовых актов, регулирующих деятельность базы практики. <p style="text-align: center;">Основной этап:</p> <ol style="list-style-type: none"> 1. Выполнение производственных заданий. <ul style="list-style-type: none"> • ознакомление с конкретными видами деятельности в

	<p>соответствии с положениями структурных подразделений и должностными инструкциями;</p> <ul style="list-style-type: none"> • ознакомление с задачами отдела/службы организации базы практики; • сбор информации и материалов в соответствии с заданием на практику; • выполнение заданий, поставленных руководителями практики; • обработка, систематизация и анализ фактического и теоретического материала. <p>2. Подготовка материалов для отчёта по практике:</p> <ul style="list-style-type: none"> • разработка и исследование математических моделей процессов и объектов, возникающих в системах компьютерной безопасности; • разработка и анализ эффективности вычислительных алгоритмов, реализующих процессы обработки информации в компьютерных системах; • проведение компьютерных экспериментов, демонстрирующих работоспособность компьютерных программ, и получение статистических оценок эффективности разработанных моделей и алгоритмов. <p>3. Ведение дневника практики.</p> <p style="text-align: center;">Заключительный этап:</p> <ol style="list-style-type: none"> 1. Выявление возможных недостатков в работе подразделения – места прохождения практики, их оценка и разработка предложений по совершенствованию существующего порядка работы, а также по внедрению новых методов работы. 2. Подготовка отчета о прохождении практики, представления отчета по практике и прилагаемых документов для защиты. 3. Защита отчёта по практике
Разработчики	Доцент ИФМН и ИТ БФУ им. И.Канта, к.т.н., доцент <i>Ветров Игорь Анатольевич</i>

АННОТАЦИЯ рабочей программы «Производственная практика (научно-исследовательская работа)» для студентов 6 курса очной формы обучения специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация (степень) выпускника: <i>специалист</i>	
Вид практики	Производственная практика
Тип практики	Научно-исследовательская работа
Способ проведения практики	Стационарная
Форма проведения практики	Непрерывная
Цель практики	<p>Целью НИР является освоение студентом методики проведения всех этапов научно-исследовательской работы – от постановки задачи исследования; через исследование и разработку средств и систем защиты информации, доказательный анализ защищённости компьютерных систем от вредоносных программно-технических воздействий в условиях существования угроз в информационной сфере; через рациональное планирование эксплуатации систем управления и обеспечения информационной безопасности; до подготовки отчётов по теме или её разделу.</p> <p>Задачами НИР являются:</p> <ol style="list-style-type: none"> 1) развитие способностей студента к самостоятельной аналитической работе; 2) освоение процедур планирования, проведения и анализа результатов научных исследований в соответствии с заданием на НИР; 3) формирование и развитие у студентов устойчивого интереса к профессиональной деятельности, потребности в самообразовании; 4) разработка научной (теоретической части) выпускной квалификационной работы в соответствии с выбранной темой.
Компетенции, формируемые в результате освоения практики	<p style="text-align: center;">ОПК-3</p> <p>Способен, на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности</p> <p style="text-align: center;">ОПК-7</p> <p>Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования</p>

	<p style="text-align: center;">ОПК-8</p> <p>Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей</p> <p style="text-align: center;">ОПК-9</p> <p>Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации</p> <p style="text-align: center;">ОПК-11</p> <p>Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации</p>
<p>Результаты освоения образовательной программы (ИДК)</p>	<p>ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации.</p> <p>ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации.</p> <p>ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.</p> <p>ОПК-7.1. Разрабатывает программы на языках высокого и низкого уровня.</p> <p>ОПК-7.1. Применяет известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач.</p> <p>ОПК-7.1. Осуществляет обоснованный выбор инструментария программирования и способов организации программ.</p> <p>ОПК-8.1. Знает принципы работы с научной литературой, методы поиска научно-технической информации.</p> <p>ОПК-8.2. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов.</p> <p>ОПК-8.3. Обладает навыками решения профессиональных задач с широким использованием актуальной научно-технической литературы.</p> <p>ОПК-9.1. Знает методы защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки</p>

	<p>по техническим каналам, сетей и систем передачи информации.</p> <p>ОПК-9.2. Умеет решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.</p> <p>ОПК-9.3. Владеет навыками решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.</p> <p>ОПК-11.1. Знает меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты.</p> <p>ОПК-11.2. Способен формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности.</p> <p>ОПК-11.3. Владеет навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.</p>
<p>Знания, умения и навыки, получаемые в процессе прохождения практики</p>	<p>В результате прохождения производственной практики (научно-исследовательская работа) обучающийся должен:</p> <p style="text-align: center;">знать:</p> <ul style="list-style-type: none"> - необходимые математические методы для решения задач обеспечения защиты информации; - методику разработки программ на языках высокого и низкого уровня; - принципы работы с научной литературой, методы поиска научно-технической информации; - методы защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации; - меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты; <p style="text-align: center;">уметь:</p> <ul style="list-style-type: none"> - применять совокупность необходимых математических методов для решения задач обеспечения защиты информации;

	<ul style="list-style-type: none"> - применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач; - осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов; - решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации; - формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности; <p style="text-align: center;">владеть:</p> <ul style="list-style-type: none"> - разработкой, обоснованием и реализацией на практике процедур решения задач обеспечения защиты информации; - обоснованным выбором инструментария программирования и способов организации навыками решения профессиональных задач с широким использованием актуальной научно-технической литературы; - навыками решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации; - навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.
<p>Структура и содержание практики</p>	<p style="text-align: center;">Организационный этап:</p> <ol style="list-style-type: none"> 1. Организационное собрание для разъяснения целей, задач, содержания и порядка прохождения НИР. 2. Обязательный инструктаж по охране труда (вводный и на рабочем месте), инструктаж по технике безопасности, пожарной безопасности. 3. Ознакомление с правилами внутреннего распорядка на базе прохождения НИР. 4. Получение и согласование индивидуального задания по прохождению НИР. 5. Составление индивидуального плана НИР совместно с научным руководителем: выбор и обоснование текущей темы исследования;

	<p>составление рабочего плана и графика выполнения исследования.</p> <p>6. Получение документации по НИР (программа НИР и дневник НИР) в сроки, определенные программой.</p> <p style="text-align: center;">Основной этап:</p> <ol style="list-style-type: none"> 1. Подготовка к проведению научного исследования: ознакомление со структурой и принципами работы исследуемых компьютерных систем, взаимосвязей между информационными потоками; постановка целей и конкретных задач; формулировка рабочих гипотез; обзор и анализ литературы по теме исследования, сбор информации. 2. Проведение экспериментального исследования: компьютерное моделирование и статистический анализ уровней защищённости компьютерных систем, вычислительной эффективности алгоритмов, качества псевдослучайных последовательностей. 3. Проведение теоретического исследования: разработка структурных схем, математических моделей, протоколов обмена информацией; анализ свойств математических моделей; анализ и разработка алгоритмов; планирование компьютерных экспериментов; компьютерное моделирование алгоритмов. 4. Обработка, систематизация и анализ полученных теоретических результатов и результатов компьютерного моделирования, проверка корректности разработанных алгоритмов; проверка работоспособности комплекса программ. 5. Анализ возможности публичного представления результатов НИР, возможности внедрения результатов исследования в проектную деятельность, инженерную практику, в производство. <p style="text-align: center;">Заключительный этап:</p> <ol style="list-style-type: none"> 1. Подготовка отчета о НИР, представления отчета по НИР и прилагаемых документов для защиты 2. Защита отчёта по практике
Разработчики	Доцент ИФМН и ИТ БФУ им. И.Канта, к.т.н., доцент <i>Ветров Игорь Анатольевич</i>

АННОТАЦИЯ рабочей программы «Производственная преддипломная практика» для студентов 6 курса очной формы обучения по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Вид практики	Производственная практика
Тип практики	Преддипломная
Способ проведения практики	Стационарная
Форма проведения практики	Непрерывная
Цель практики	<p>Целью преддипломной практики является углубление профессиональных знаний и адаптация их к условиям конкретного производства, закрепление профессиональных компетенций, приобретение дополнительного опыта практической работы, сбор и обработка материала для написания ВКР.</p> <p>Задачи преддипломной практики:</p> <ul style="list-style-type: none"> • развитие навыков студента к применению знаний и умений, полученных в результате теоретической подготовки, к выполнению практических заданий в области обеспечения компьютерной безопасности, управления информационной безопасностью, эксплуатации технических и программно-аппаратных средств защиты информации; • развитие умения анализировать существующие системы компьютерной (информационной) безопасности на предмет стойкости, эффективности и соответствия нормативным документам; • развитие навыков эскизного и технического проектирования систем (подсистем, элементов) обеспечения компьютерной (информационной) безопасности, систем управления информационной безопасностью, планирования работы систем эксплуатации технических и программно-аппаратных средств защиты информации; • завершение разработки научной (теоретической части) ВКР, а также сбор и подготовка данных для прикладной части ВКР в соответствии с выбранной темой.
Компетенции, формируемые в результате освоения практики	ОПК-2
	Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности

	<p style="text-align: center;">ОПК-3</p> <p>Способен, на основании совокупности математических методов, разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности</p> <p style="text-align: center;">ОПК-7</p> <p>Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования</p> <p style="text-align: center;">ОПК-12</p> <p>Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения</p> <p style="text-align: center;">ОПК-13</p> <p>Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности</p> <p style="text-align: center;">ОПК-15</p> <p>Способен администрировать компьютерные сети и контролировать корректность их функционирования</p> <p style="text-align: center;">ОПК-16</p> <p>Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях</p>
<p>Результаты освоения образовательной программы (ИДК)</p>	<p>ОПК-2.1. Понимает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности.</p> <p>ОПК-2.2. Выбирает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности.</p> <p>ОПК-2.3. Обладает навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности.</p> <p>ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации.</p> <p>ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации.</p> <p>ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.</p>

ОПК-7.1. Разрабатывает программы на языках высокого и низкого уровня.

ОПК-7.1. Применяет известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач.

ОПК-7.1. Осуществляет обоснованный выбор инструментария программирования и способов организации программ.

ОПК-12.1. Знает принципы и способы администрирования операционных систем, методы и алгоритмы восстановления работоспособности прикладного и системного программного обеспечения

ОПК-12.2. Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения

ОПК-12.3. Владеет навыками администрирования операционных систем и восстановления работоспособности прикладного и системного программного обеспечения

ОПК-13.1. Знает принципы функционирования программных и программно-аппаратных средств защиты информации в компьютерных системах, принципы и методы разработки их компонент, методики анализа их безопасности.

ОПК-13.2. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах

ОПК-13.3. Способен проводить анализ безопасности компонент программных и программно-аппаратных средств защиты информации в компьютерных системах

ОПК-15.1. Знает устройство, порядок администрирования и контроля функционирования компьютерных сетей.

ОПК-15.2. Умеет осуществлять администрирование и контроль корректности функционирования компьютерных сетей.

ОПК-15.3. Владеет навыками администрирования и контроля функционирования компьютерных сетей

ОПК-16.1. Знает устройство, принципы функционирования, порядок настройки, мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях.

ОПК-16.2. Умеет осуществлять мониторинг работоспособности и анализ эффективности средств защиты информации в

	<p>компьютерных системах и сетях.</p> <p>ОПК-16.3. Владеет навыками мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях.</p>
<p>Знания, умения и навыки, получаемые в процессе прохождения практики</p>	<p>В результате прохождения практики обучающийся должен:</p> <p style="text-align: center;">знать:</p> <ul style="list-style-type: none"> • современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности; • необходимые математические методы для решения задач обеспечения защиты информации; • методику разработки программ на языках высокого и низкого уровня; • принципы и способы администрирования операционных систем, методы и алгоритмы восстановления работоспособности прикладного и системного программного обеспечения; • принципы функционирования программных и программно-аппаратных средств защиты информации в компьютерных системах, принципы и методы разработки их компонент, методики анализа их безопасности; • устройство, порядок администрирования и контроля функционирования компьютерных сетей; • устройство, принципы функционирования, порядок настройки, мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях; <p style="text-align: center;">уметь:</p> <ul style="list-style-type: none"> • выбирать современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности; • применять совокупность необходимых математических методов для решения задач обеспечения защиты информации; • применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач; • администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения; • разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах; • осуществлять администрирование и контроль корректности функционирования компьютерных сетей; • осуществлять мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных

	<p>системах и сетях;</p> <p style="text-align: center;">владеть:</p> <ul style="list-style-type: none"> • навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности; • разработкой, обоснованием и реализацией на практике процедур решения задач обеспечения защиты информации; • обоснованным выбором инструментария программирования и способов организации программ; • навыками администрирования операционных систем и восстановления работоспособности прикладного и системного программного обеспечения; • способами анализа безопасности компонент программных и программно-аппаратных средств защиты информации в компьютерных системах; • навыками администрирования и контроля функционирования компьютерных сетей; • навыками мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях.
<p>Структура и содержание практики</p>	<p style="text-align: center;">Организационный этап:</p> <ol style="list-style-type: none"> 1. Определение базы прохождения практики. 2. Организационное собрание для разъяснения целей, задач, содержания и порядка прохождения практики. 3. Обязательный инструктаж по охране труда (вводный и на рабочем месте), инструктаж по технике безопасности, пожарной безопасности. 4. Ознакомление с правилами внутреннего распорядка на базе прохождения практики. 5. Получение и согласование индивидуального задания по прохождению практики. 6. Разработка и утверждение индивидуальной программы практики и графика выполнения исследования. 7. Получение документации по практике (программы практики, индивидуального задания на практику, плана-графика прохождения практики и дневника практики с направлением на практику) в сроки, определенные программой. 8. Изучение правовых основ, базовых нормативных и локальных правовых актов, регулирующих деятельность базы практики. <p style="text-align: center;">Основной этап:</p> <ol style="list-style-type: none"> 1. Выполнение производственных заданий. <ul style="list-style-type: none"> • ознакомление с конкретными видами деятельности в соответствии с положениями структурных подразделений и

	<p>должностными инструкциями;</p> <ul style="list-style-type: none"> • ознакомление с задачами отдела/службы организации базы практики; • сбор информации и материалов в соответствии с заданием на практику; • выполнение заданий, поставленных руководителями практики; • обработка, систематизация и анализ фактического и теоретического материала. <p>2. Подготовка материалов для ВКР:</p> <ul style="list-style-type: none"> • разработка и исследование математических моделей процессов и объектов, возникающих в системах компьютерной безопасности; • разработка и анализ эффективности вычислительных алгоритмов, реализующих процессы обработки информации в компьютерных системах; • проведение компьютерных экспериментов, демонстрирующих работоспособность компьютерных программ, и получение статистических оценок эффективности разработанных моделей и алгоритмов. <p>3. Введение дневника практики.</p> <p style="text-align: center;">Заключительный этап:</p> <ol style="list-style-type: none"> 1. Выявление возможных недостатков в работе подразделения – места прохождения практики, их оценка и разработка предложений по совершенствованию существующего порядка работы, а также по внедрению новых методов работы. 2. Подготовка отчета о прохождении практики, представления отчета по практике и прилагаемых документов для защиты. 3. Защита отчёта по практике
Разработчики	<p>Доцент ИФМН и ИТ БФУ им. И.Канта, к.т.н., доцент <i>Ветров Игорь Анатольевич</i></p>