Минобрнауки России
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A29CA99D98126F4EB57F6F989D713C88
Владелец: Василенко Виталий Николаевич
Действителен: с 07.07.2022 до 30.09.2023

УТВЕРЖДАЮ
Проректор по учебной работе

_____ Василенко В.Н.
(подпись) (Ф.И.О.)

«26» мая 2022

ПРОГРАММА ПРАКТИКИ

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА
ПРАКТИКА ПО ПОЛУЧЕНИЮ ПРОФЕССИОНАЛЬНЫХ УМЕНИЙ И ОПЫТА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Безопасность открытых информационных систем

Квалификация (степень) выпускника

специалист по защите информации

Разработчик _____ _____ _____Скрыпников А.В._____
(подпись) (дата) (Ф.И.О.)

СОГЛАСОВАНО:

Заведующий кафедрой _____информационной безопасности_____
(наименование кафедры, являющейся ответственной за данное направление подготовки, профиль)

_____ _____ _____Скрыпников А.В._____
(подпись) (дата) (Ф.И.О.)

1. Цели практики

Целями производственной практики является изучение опыта создания и применения защищенных информационных технологий и систем для решения реальных задач организационной, управленческой или научной деятельности в условиях конкретных производств, организаций или корпораций; приобретение навыков практического решения задач защиты информации на рабочем месте.

2. Задачи практики

– углубление знаний, полученных в ходе обучения, развитие навыков их применения в практической области защиты информации;

– усвоение и закрепление навыков самостоятельной работы и самостоятельного решения поставленных задач;

– развитие навыков администрирования подсистем информационной безопасности.

Объектами профессиональной деятельности специалистов являются:

– автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;

– информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно- технологические ресурсы, подлежащие защите;

– технологии обеспечения информационной безопасности автоматизированных систем; системы управления информационной безопасностью автоматизированных систем.

Место практики в структуре образовательной программы

3.1. Производственная практика (по получению профессиональных умений и опыта профессиональной деятельности) относится к базовой части Блока 2 «Практики» образовательной программы.

Практика является важнейшей составной частью учебного процесса подготовки специалистов и проводится на основании учебного плана по направлению 10.05.03 – Информационная безопасность автоматизированных систем, в соответствии с требованиями Федерального Государственного образовательного стандарта высшего образования.

3.2. Для успешного прохождения практики необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: «Экология», «Программно-аппаратные средства обеспечения информационной безопасности», «Организационно-правовое обеспечения информационной безопасности», «Защита web-сайтов», «Учебная практика (по получению первичных профессиональных умений и навыков научно-исследовательской деятельности)».

Для освоения производственной практики студент должен:

– знать законодательные и нормативные нормы и регламенты организации работы с персоналом по защите персональных данных;

– уметь применять технические и программные средства защиты информации;

– владеть информационными технологиями защиты информации на предприятии.

3.3. Знания, умения и навыки, сформированные при прохождении практики, необходимы для успешного освоения последующих дисциплин «Преддипломная практика», «Защита конфиденциальной информации», «Надежность информационных систем».

4. Перечень планируемых результатов обучения при прохождении практики

Процесс прохождения практики направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению подготовки:

– способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1);

– способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);

– способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);

– способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах (ОПК-4);

– способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5);

– способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6);

– способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-7);

– способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8);

– способностью осуществлять поиск, изучение, обобщение и систематизацию научно- технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);

– способностью создавать и исследовать модели автоматизированных систем (ПК-2);

– способностью проводить анализ защищенности автоматизированных систем (ПК-3);

– способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);

– способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);

– способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);

– способностью разрабатывать научно-техническую документацию, готовить научно- технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);

– способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);

– способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);

– способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);

– способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);

– способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);

– способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);

– способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК- 14);

– способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);

– способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);

– способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);

– способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);

– способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

– способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);

– способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

– способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

– способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

– способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);

– способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);

– способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);

– способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);

– способностью управлять информационной безопасностью автоматизированной системы (ПК-28);

– способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем (ПСК-4.1);

– способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем (ПСК-4.2);

– способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы (ПСК-4.3);

– способностью участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы (ПСК-4.4);

– способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем (ПСК-4.5).

В результате прохождения практики обучающийся должен:

Знать:

– основные понятия и задачи векторной алгебры и аналитической геометрии (ОПК-1);

– современные технологии и методы программирования (ОПК-3);

– формы и способы представления данных в персональном компьютере (ОПК-4);

– методы научных исследований в профессиональной деятельности (ОПК-5);

– основы организационного и правового обеспечения информационной безопасности (ОПК-6);

– технику безопасности при работе с приборами и оборудованием для защиты информации (ОПК-7);

– основные технические и программные средства защиты информации, используемые на предприятии (ОПК-8);

– предъявляемые в организациях требования к специалистам, работающим в области защиты информации (ПК-1);

– основные технологии защиты информации, используемые на предприятии (ПК-2);

– средства обеспечения безопасности данных (ПК-3);

– источники и классификацию угроз информационной безопасности (ПК-4);

– основные риски информационной безопасности (ПК-5);

– мировые и российские стандарты в области информационной безопасности (ПК-6);

– принципы организации документирования разработки, процесса сопровождения программного обеспечения (ПК-7);

– характеристики каналов передачи данных (ПК-10);

– принципы построения систем защиты информации (ПК-11);

– компоненты системы управления информационной безопасностью автоматизированной системы (ПК-12);

– методы и средства проектирования средств защиты информации (ПК-13);

– процесс сопровождения программного обеспечения (ПК-14);

– правовые акты по аттестации объектов информатизации и сертификации средств защиты информации (ПК-15);

– нормативную документацию в области аттестации автоматизированных систем (ПК-16);

– функции межсетевых экранов, профили защиты для межсетевых экранов (ПК-17);

– методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем (ПК-20);

– разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

– задачи систем анализа защищенности в защите открытых систем (ПК-22);

– состав информации ограниченного доступа организации (ПК-23);

– слабости системных утилит, команд и сетевых сервисов (ПК-24);

– методы, принципы, процедуры и службы администрирования информационных систем (ПК-26);

– основные протоколы компьютерных сетей (ПК-27);

– технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования (ПК-28);

– комплексном подходе к построению эшелонированной защиты для автоматизированных систем (ПСК-4.1);

– понятия информационной безопасности, защиты информации, назначение и основные возможности систем защиты информации (ПСК-4.2);

– основные компоненты архитектуры мобильных платформ (ПСК-4.3);

– терминологию и системный подход построения защищенных открытых информационных систем (ПСК-4.4);

– принципы декодирования HTTP (ПСК-4.5).

Уметь:

– определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач (ОПК-1);

– применять при решении профессиональных задач с использованием вычислительной техники соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации (ОПК-2);

– строить логические и правильные программы (ОПК-3);

– применять средства восстановления системы после сбоя, чистки и дефрагментации диска (ОПК-4);

– проводить комплексное проектировать структуру и архитектуру программного обеспечения с использованием современных методологий (ОПК-5);

– применять нормативные правовые акты, руководящие и методические документы, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении на различных стадиях их жизненного цикла (ОПК-6);

– работать с офисной техникой и специализированным оборудованием с учетом требований техники безопасности (ОПК-7);

– пользоваться приборами выявления каналов утечки информации, обнаружения подслушивающих устройств и приборов незаконного съема информации, локализации действия средств несанкционированного доступа (ОПК-8);

– работать со специализированными прикладными программами, инструментальной системой программирования и ресурсами Интернет (ПК-1);

– применять основные законы и нормативные документы в области информационной безопасности (ПК-3);

– проводить мониторинг угроз безопасности компьютерных сетей (ПК-4);

– планировать политику безопасности операционных систем (ПК-5);

– применять на практике методы анализа электрических цепей (ПК-6);

– пользоваться нормативными документами но противодействию технической разведке (ПК-7);

– проводить анализ проектных решений по обеспечению информационной безопасности (ПК-8);

– формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения (ПК-9);

– анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей (ПК- 10);

– участвовать в разработке политики информационной безопасности (ПК-11);

– проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов (ПК-13);

– участвовать в контрольных проверках работоспособности применяемых программно-аппаратных средств (ПК-14);

– участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации (ПК-15);

– соблюдать правила вежливости и культуры поведения в профессиональной деятельности давать нравственную оценку коррупционным проявлениям и другим нарушениям норм профессиональной этики (ПК-18);

– участвовать в разработке предложений по совершенствованию системы управления информационной безопасностью (ПК-19);

– участвовать в коллективной разработке проектов документов по обеспечению информационной безопасности (ПК-21);

– применять принципы формирования политики информационной безопасности (ПК-22);

– применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем (ПК-23);

– применять математические методы при решении профессиональных задач моделирования повышенной сложности (ПК-24);

– использовать частные и обобщенные модели систем комплексной защиты информации (ПК-25);

– участвовать в администрировании подсистемы информационной безопасности (ПК-26);

– разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных (ПК-27);

– участвовать в работе коллектива по управлению информационной безопасностью организации (ПК-28);

– открывать и закрывать общий доступ к информации в локальной сети (ПСК-4.2);

– устранять источники угроз безопасности мобильных систем и приложений (ПСК-4.3);

– проектировать взаимодействия многомашинных информационных систем, используя стандартные протоколы эталонной модели (ПСК-4.4);

– создавать CGI, ISAPI и WEB приложения (ПСК-4.5).

Владеть:

– навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач (ОПК-1);

– расчетными формулами, компьютерными программами при решении математических задач (ОПК-2);

– составления программ по разработанным алгоритмам (ОПК-3);

– навыками работы с современными информационными технологиями для поиска информации (ОПК-4);

– навыками организации и обеспечения режима секретности (ОПК-6);

– навыками работы с измерительными приборами и типовым оборудованием для защиты информации (ОПК-7);

– методиками проведения аналитической работы по предупреждению утечки конфиденциальной информации (ОПК-8);

– применения руководящих и нормативных документов по инженерно-технической защите информации (ПК-1);

– навыками проектирования программного обеспечения с использованием средств автоматизации (ПК-2);

– навыками анализа основных узлов устройств современных автоматизированных систем (ПК-3);

– навыками программирования в профессиональной деятельности (ПК-4);

– навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем (ПК-5);

– навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств (ПК-6);

– навыками разработки, документирования, тестирования и отладки программного обеспечения (ПК-7);

– профессиональной терминологией в области информационной безопасности (ПК-8);

– способностью учувствовать в разработке защищенных автоматизированных систем (ПК-9);

– планирования политики безопасности операционных систем (ПК-11);

– навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей (ПК-12);

– навыками проведения экспериментально-исследовательских работ при сертификации средств защиты информации (ПК-15);

– навыками использования измерительного оборудования при экспериментальном исследовании электронной аппаратуры (ПК-16);

– выбора и использования архитектурных особенностей вычислительных систем различных классов (ПК-17);

– навыками конструктивного общения в процессе профессиональной деятельности (ПК-18);

– методами формирования требований по защите информации (ПК-19);

– навыками эксплуатации автоматизированной системы с учетом требований информационной безопасности (ПК-20);

– навыками работы с сетевыми сканерами, сканерами безопасности (ПК-25);

– средствами SQL Server для администрирования удаленных баз данных (ПК-26);

– навыками применения различных методов и мер обеспечения доверия к информационной безопасности: лицензирование, аккредитация, оценка и подтверждение соответствия (ПСК-4.1);

– навыками программирования простейших методов шифрования-дешифрования (ПСК- 4.3);

– навыками оценивания стойкости различных паролей (ПСК-4.4);

– навыками формирования ключей шифрования с заданной стойкостью (ПСК-4.5).

5. Способы и форма(ы) проведения практики

Практика является стационарной и выездной, и может проводиться в отделах защиты информации, отделах АСУ, вычислительных центрах, отделах, занимающихся разработкой и внедрением программного обеспечения, проектированием, монтажом и поддержкой вычислительных сетей, отделах, занимающихся разработкой, продвижением и поддержкой web-сайтов.

6. Структура и содержание практики

6.1. Содержание разделов практики

1) аналитический обзор нормативно-правовой документации предприятия по обеспечению информационной безопасности, законодательно-правовой базой по защите персональных данных сотрудников подразделения, на котором проводится практика;

2) описание видов, методов, средств информационной защиты, применяемых на предприятии;

3) выполнение установки, настройки или эксплуатации компонентов системы обеспечения информационной безопасности согласно индивидуальным задачам производственной практики.

6.2. Распределение часов по семестрам и видам работ по практике

Общая трудоемкость прохождения практики составляет 3 з.е., 108 академических часов, 2 недели. Контактная работа обучающегося (КРо) составляет 72 ч. Иные формы работы – 36 ч.

7. Формы промежуточной аттестации (отчётности по итогам практики)

Отчет и дневник практик необходимо составлять во время практики по мере обработки того или иного раздела программы. По окончании практики и после проверки отчета руководителями практики от производства и кафедры, студент защищает отчет в установленный срок перед комиссией, назначаемой заведующим кафедрой.

По окончании срока практики, руководители практики от Университета доводят до сведения обучающихся график защиты отчетов по практике.

В течение двух рабочих дней после окончания срока практики обучающийся предоставляет на кафедру отчет и дневник по практике, оформленные в соответствии с требованиями, установленными программой практики с характеристикой работы обучающегося, оценками прохождения практики и качества компетенций, приобретенных им в результате прохождения практики, данной руководителем практики от организации.

В двухнедельный срок после начала занятий обучающиеся обязаны защитить его на кафедральной комиссии, график работы которой доводится до сведения студентов.

Аттестация по итогам практики проводится на основании оформленного в соответствии с установленными требованиями письменного отчета и характеристики руководителя практики от организации. По итогам аттестации выставляется оценка (отлично, хорошо, удовлетворительно, неудовлетворительно). **Отчет и дневник** по практике обучающийся сдает руководителю практики от Университета.

8. Оценочные материалы для промежуточной аттестации обучающихся по практике

8.1. Оценочные материалы (ОМ) для практики включает в себя:

– перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;

– описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;

– типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы;

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

8.2. Для каждого результата обучения по практике определяются показатели и критерии оценивания сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

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

При выполнении программы практики студент может использовать учебно-методическое и информационное обеспечение дисциплин учебного плана, предшествующих выполнению программы практики.

Кроме того, необходимо использовать материалы профессиональных периодических изданий и иные информационные ресурсы.

1. Технологии защиты информации в компьютерных сетях / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 369 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=428820. – Текст : электронный.

2. Системы защиты информации в ведущих зарубежных странах : учебное пособие / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский ; науч. ред. В. И. Аверченков. – 5-е изд., стер. – Москва : ФЛИНТА, 2021. – 224 с. : ил., схем. – (Организация и технология защиты информации). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93351. – Текст : электронный.

3. Костин, В. Н. Методы и средства защиты компьютерной информации: криптографические методы для защиты информации : учебное пособие / В. Н. Костин. – Москва : МИСиС, 2018. – 40 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=497572. – Текст : электронный.

4. Скрипник, Д. А. Общие вопросы технической защиты информации / Д. А. Скрипник. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 425 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429070. – Текст : электронный.

5. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 256 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480636 . – Текст : электронный.

10. Образовательные, научно-исследовательские и научно-производственные технологии, используемые на практике

Информационно-развивающие технологии:

– использование мультимедийного оборудования при проведении практики;

– получение студентом необходимой учебной информации под руководством преподавателя или самостоятельно;

– метод IT - использование в учебном процессе системы автоматизированного проектирования.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Перечень программного обеспечения и информационных справочных систем:

1. Microsoft Office Professional Plus 2010;
2. Microsoft Office Professional Plus 2013;
3. Microsoft Office 2007;
4. Среда разработки MS Visual Studio;
5. СУБД MS SQL Server;
6. Программный пакет «Crypton LITE»;
7. Kerio WinRoute FireWall;
8. сканер безопасности «XSpider»;
9. Страж NT (версия 3.0);
10. Ревизор Сети (10 IP-адресов);
11. Ревизор-2 XP, Ревизор-1 XP;
12. Lazarus;
13. «Российское образование» - федеральный портал https://www.edu.ru/;
14. Научная электронная библиотека https://elibrary.ru/defaultx.asp;
15. Национальная исследовательская компьютерная сеть России https://niks.su/;
16. Информационная система «Единое окно доступа к образовательным ресурсам» http://window.edu.ru/;
17. Электронная библиотека ВГУИТ http://biblos.vsuet.ru/megapro/web;
18. Сайт Министерства науки и высшего образования РФ https://minobrnauki.gov.ru/;
19. Портал открытого on-line образования https://npoed.ru/;
20. Электронная информационно-образовательная среда ФГБОУ ВО «ВГУИТ» https://education.vsuet.ru/.

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

Для проведения практики используется материально-техническая база кафедры информационной безопасности, ее аудиторный фонд, соответствующий санитарным, противопожарным нормам и требованиям техники безопасности. Кафедра располагает наличием компьютерных классов (аудиториями (а. 332а, 420, 424), оснащенными в каждой аудитории 12 ПК Intel Core 2 Duo персональных компьютеров) с выходом в сеть «Интернет» и установленным лицензионным программным обеспечением (Microsoft Windows 8.1, Microsoft Office 2013, AutoCAD, САПР КОМПАС и др.).

Документ составлен в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем.