

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

УТВЕРЖДАЮ
Проректор по учебной работе

(подпись) Василенко В.Н.
(Ф.И.О.)

«26» мая 2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Безопасность открытых информационных систем

Квалификация (степень) выпускника

специалист по защите информации

Разработчик _____
(подпись) (дата) (Ф.И.О.)

СОГЛАСОВАНО:

Заведующий кафедрой _____ информационной безопасности _____
(наименование кафедры, являющейся ответственной за данное направление подготовки, профиль)

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

1 Цели и задачи дисциплины

Целью дисциплины «Основы информационной безопасности» является формирование основ компетентности в обеспечении информационной безопасности государства.

Задачи дисциплины:

- развитие системного мышления в области обеспечения информационной безопасности государства;
- обучение методологии создания систем защиты информации, методам оценки защищенности и обеспечения информационной безопасности компьютерных систем;
- освоение обучаемым социальной роли специалиста по защите информации.

Объектами профессиональной деятельности 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.

2 Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины в соответствии с предусмотренными компетенциями обучающийся должен:

| № п/п | Код компетенции | Содержание компетенции (результат освоения) | В результате изучения учебной дисциплины обучающийся должен: | | |
|-------|-----------------|---|--|---|---|
| | | | знать | уметь | владеть |
| 1 | ОПК-6 | способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия | основные понятия защиты информации | работать в коллективе, толерантно воспринимая социальные, культурные и иные различия | устойчивыми навыками работы с различными социальными группами в сфере системы безопасности |
| 2 | ПК-7 | способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ | цели, задачи, принципы и основные направления обеспечения информационной безопасности государства; основные термины по проблематике информационной безопасности; методологию создания систем защиты информации | выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации | навыками разработки политики информационной безопасности автоматизированных систем |
| 3 | ПК-11 | способностью разрабатывать политику информационной безопасности автоматизированной системы | перспективные направления развития средств и методов защиты информации, содержание информационной войны, методы и средства ее ведения | пользоваться современной научно-технической информацией по исследуемым проблемам и задачам | навыками проектирования системы управления информационной безопасностью автоматизированной системы, навы- |

| | | | | | |
|--|--|--|--|--|---|
| | | | | | ками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем |
|--|--|--|--|--|---|

3 Место дисциплины в структуре ОП ВО

Дисциплина «Основы информационной безопасности» относится к блоку 1 ОП и ее базовой части. Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплины «Компьютерная и инженерная графика».

Дисциплина является предшествующей для изучения дисциплин, прохождения практик:

- Управление информационной безопасностью;
- Разработка и эксплуатация защищенных автоматизированных систем;
- Администрирование в информационных системах;
- Аудит информационных технологий и систем обеспечения информационной безопасности;
- Защита конфиденциальной информации;
- Организационное и правовое обеспечение информационной безопасности;
- Учебная практика, практика по получению первичных умений и навыков научно-исследовательской деятельности;
- Производственная практика, практика по получению профессиональных умений и опыта профессиональной деятельности;
- Производственная практика, преддипломная практика; защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

4 Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет 6 зачетных единиц.

| Виды учебной работы | Всего часов | Семестр |
|---|--------------|--------------|
| | | 4 |
| | акад. | акад. |
| Общая трудоемкость дисциплины | 216 | 216 |
| Контактная работа, в т.ч. аудиторные занятия | 73,9 | 73,9 |
| Лекции | 36 | 36 |
| <i>в том числе в форме практической подготовки</i> | – | – |
| Практические занятия (ПЗ) | 36 | 36 |
| <i>в том числе в форме практической подготовки</i> | 36 | 36 |
| Консультации текущие | 1,9 | 1,9 |
| Вид аттестации – зачет | 0,1 | 0,1 |
| Самостоятельная работа | 142,1 | 142,1 |
| Подготовка доклада с презентацией | 35 | 35 |
| Расчетно-практическая работа | 70,1 | 70,1 |
| Тестирование | 37 | 37 |

5 Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1 Содержание разделов дисциплины

| № п/п | Наименование разделов дисциплины | Содержание раздела |
|-------|---|--|
| 1 | Введение в проблему информационной безопасности. Основные понятия защиты информации. | Понятие информационной безопасности. Основные составляющие. Терминология информационной безопасности. Распространение объектно-ориентированного подхода на информационную безопасность. |
| 2 | Законодательные основы информационной безопасности. Стандарты и спецификации в области информационной безопасности. | Законодательное регулирование информационной безопасности. Рассмотрение международных и национальных стандартов и спецификаций в области информационной безопасности. «Оранжевая книга» как оценочный стандарт. Механизмы безопасности. Классы безопасности. Рассматриваются руководящие документы ФСТЭК России. |
| 3 | Угрозы информационной безопасности. Подходы к построению систем защиты информации. | Рассматриваются угрозы информационной безопасности. Описываются административный, процедурный, программно-технический уровни обеспечения информационной безопасности. Идентификация, аутентификация и управление доступом. Криптографические методы защиты информации. |

5.2 Разделы дисциплины и виды занятий

| № п/п | Наименование раздела дисциплины | Лекции, час | ПЗ, час | СР, час |
|-------|---|-------------|---------|---------|
| 1 | Введение в проблему информационной безопасности. Основные понятия защиты информации. | 10 | 10 | 35 |
| 2 | Законодательные основы информационной безопасности. Стандарты и спецификации в области информационной безопасности. | 13 | 13 | 70,1 |
| 3 | Угрозы информационной безопасности. Подходы к построению систем защиты информации. | 13 | 13 | 37 |

5.2.1 Лекции

| № п/п | Наименование раздела дисциплины | Тематика лекционных занятий | Трудоемкость, час |
|-------|---|---|-------------------|
| 1 | Введение в проблему информационной безопасности. Основные понятия защиты информации. | Понятие информационной безопасности. Основные составляющие. Важность проблемы. Терминология и основные понятия защиты информации. Распространение объектно-ориентированного подхода на информационную безопасность. | 10 |
| 2 | Законодательные основы информационной безопасности. Стандарты и спецификации в области информационной безопасности. | Законодательный уровень информационной безопасности. Мировые стандарты в области информационной безопасности. Российские стандарты в области информационной безопасности. Спецификации в области информационной безопасности. Особенности нормотворческой деятельности в области информационной безопасности. | 13 |
| 3 | Угрозы информационной безопасности. Подходы к построению систем защиты информации. | Угрозы информационной безопасности. Административный уровень информационной безопасности. Управление рисками. Процедурный уровень информационной | 13 |

| | | | |
|--|--|--|--|
| | | безопасности. Основные программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация и управление доступом. Криптографические методы защиты информации. | |
|--|--|--|--|

5.2.2 Практические занятия

| № п/п | Наименование раздела дисциплины | Тематика практических занятий | Трудоемкость, час |
|-------|---|---|-------------------|
| 1 | Введение в проблему информационной безопасности. Основные понятия защиты информации. | Метод анализа конкретных ситуаций Администрирование, политика и компоненты системы безопасности | 10 |
| 2 | Законодательные основы информационной безопасности. Стандарты и спецификации в области информационной безопасности. | Разработка приказов (инструкций) регламентирующих сферу информационной безопасности на предприятии. | 13 |
| 3 | Угрозы информационной безопасности. Подходы к построению систем защиты информации. | Изучение и отработка программно-технических мер обеспечения информационной безопасности. | 13 |

5.2.3 Лабораторный практикум не предусмотрен

5.2.4 Самостоятельная работа обучающихся (СРО)

| № п/п | Наименование раздела дисциплины | Вид СРО | Трудоемкость, час |
|-------|--|---|-------------------|
| 1 | Введение в проблему информационной безопасности. Основные понятия защиты информации. Законодательные основы информационной безопасности. Стандарты и спецификации в области информационной безопасности. | Подготовка доклада с визуальным представлением средствами PowerPoint | 35 |
| 2 | Угрозы информационной безопасности. Подходы к построению систем защиты информации. Введение в проблему информационной безопасности. Основные понятия защиты информации. | Расчетно-практическая работа «Создание алгоритма и программы кодирования и декодирования методом ШеннонаФэно» | 70,1 |
| 3 | Законодательные основы информационной безопасности. Стандарты и спецификации в области информационной безопасности. | Тестирование | 37 |

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

Основы информационной безопасности (введение в профессию) [Текст] : учебное пособие для студ. по направлению "Информационная безопасность" / А. О. Горбенко. СПб. : ИЦ Интермедия, 2016. 336 с. ISBN 978-5-4383-0136-3 : 622-00. <http://biblos.vsuet.ru/MegaPro/Web/SearchResult/MarcFormat/99428>

Ярочкин, В. Безопасность информационных систем / В. Ярочкин. М.: Ось-89, 2016. – 320 с.

Степанов, Е. А. Информационная безопасность и защита информации. Учебное пособие / Е. А. Степанов, И.К. Корнеев. М.: ИНФРА-М, 2017. 304 с.

6.2 Дополнительная литература

Партыка, Т. Л. Информационная безопасность / Т. Л. Партыка, И. И. Попов. М.: Форум, Инфра-М, 2016. 368 с.

Мельников, В.П. Информационная безопасность и защита информации / В. П. Мельников. М.: Академия (Academia), 2016. 282 с.

Информационная безопасность [Текст]: словарь по терминологии. – Воронеж, 2015. – 180 с. – ISBN 978-5-44200-324-6.

Информационная безопасность открытых систем. В 2 томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников и др. Москва: Машиностроение, 2016. 536 с.

Гафнер, В.В. Информационная безопасность: Учебное пособие / В. В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

Основы информационной безопасности [Электронный ресурс]: методические указания для самостоятельной работы для студентов, обучающихся по направлению 10.05.03– «Информационная безопасность автоматизированных систем», очной формы обучения / А. В. Скрыпников, Е. В. Чернышова ; ВГУИТ, Кафедра информационной безопасности. Воронеж : ВГУИТ, 2016. 20 с. <http://biblos.vsuet.ru/ProtectedView/Book/ViewBook/>

6.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

| Наименование ресурса сети «Интернет» | Электронный адрес ресурса |
|---|---|
| «Российское образование» федеральный портал | https://www.edu.ru/ |
| Научная электронная библиотека | https://elibrary.ru/defaultx.asp |
| Национальная исследовательская компьютерная сеть России | https://niks.su/ |
| Информационная система «Единое окно доступа к образовательным ресурсам» | http://window.edu.ru/ |
| Электронная библиотека ВГУИТ | http://biblos.vsuet.ru/megapro/web |
| Сайт Министерства науки и высшего образования РФ | https://minobrnauki.gov.ru/ |
| Портал открытого on-line образования | https://npoed.ru/ |
| Электронная информационно-образовательная среда ФГБОУ ВО «ВГУИТ» | https://education.vsuet.ru/ |

6.5 Методические указания для обучающихся по освоению дисциплины

Методические указания для обучающихся по освоению дисциплин (модулей) в ФГБОУ ВО ВГУИТ [Электронный ресурс] : методические указания для обучающихся на всех уровнях высшего образования / М. М. Данылиев, Р. Н. Плотникова; ВГУИТ, Учебнометодическое управление. Воронеж : ВГУИТ, 2016. – Режим доступа : <http://biblos.vsuet.ru/MegaPro/Web/SearchResult/MarcFormat/100813>. Загл. с экрана

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

Microsoft Office, NetBeans, Wireshark, BackTrack Linux, Avast; локальная сеть университета и глобальная сеть Internet.

7. Материально-техническое обеспечение дисциплины

| | | |
|---|--|---|
| <p>Лекционные аудитории, оснащенные мультимедийной техникой</p> | <p>Аудио-визуальная система лекционных аудиторий (мультимедийный проектор, экран, усилитель мощности звука, акустические системы, микрофоны, устройство коммутации, сетевой коммутатор для подключения к компьютерной сети (Интернет))</p> | |
| <p>Аудитории для проведения лабораторных занятий</p> | <p>Ауд. 332а: Комплекты мебели для учебного процесса. ПЭВМ – 12 (компьютер Core i5-4570), стенды – 5 шт. Ауд. 424: Комплекты мебели для учебного процесса. ПЭВМ – 12: рабочая станция Регард РДЦБ.; стенды – 3 Ауд. 420: Комплекты мебели для учебного процесса. ПЭВМ-11 (компьютер Core i5-4460), проектор Acer projector X1383WH, экран, стенды – 5 шт., блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-РЗ.1»; система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной); портативный обнаружитель закладок Protect1203 (переносной); устройство активной защиты информации «ВЕТОМ»; электронный замок Samsung SHS2920</p> | <p>Ауд.332а: ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Вебредактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc, Draw, Impress, Math, Writer. Персональная бухгалтерия HomeBank. Словарь Star Dict. iTest. VM Maxima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиаплеер Parole. Редактор тергов Easy TAG. Stath Studio. Pinta. Веб-браузер Mozilla Firefox. Графический редактор. FP – free Pascal. Ауд.424: ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Вебредактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc, Draw, Impress, Math, Writer. Персональная бухгалтерия HomeBank. Словарь Star Dict. iTest. VM Maxima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиаплеер Parole. Редактор тергов Easy TAG. Stath Studio. Pinta. Веб-браузер Mozilla Firefox. Графический редактор. FP – free Pascal. Ауд.420: Microsoft Windows 7 (64 разрядная) Microsoft Office (standart) 2007; Microsoft Access 2007; Microsoft Project 2007; Microsoft Share Point 2007; Microsoft Visio 2007; Microsoft SQL server 2008; 1С Предприятие Лицензия; 7-Zip File Manager (архиватор); Adobe Acrobat Reader; Adobe Flash Player; FAR file manager; Google Chrome; Java TM 7 (64-bit); K-Lite Codec Pack; Mozilla Firefox; Oracle VM VirtualBox; Sublime Text; Symantec Endpoint Protection 12 (Заменен на AVP Kaspersky); VMWare Player; Антивирус “Зоркий глаз”; Lazarus; SmathStudio; NanoCAD; Gimp (графический редактор, аналог Photoshopy); Avidemux (видео редактор); Virtual Dub (видео редактор); Free Pascal; Страж NT вер.3.0 Сертификат ФСТЭК № 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК № 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК № 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК №1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК №3413 02.06.2015 г.; СЗИ Панцирь К Сертификат ФСТЭК №1973 09.12.2015 г.; СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК №2720 25.09.2015; СЗИ Dallas Lock 8.0</p> |

| | | |
|---|---|---|
| Аудитория для самостоятельной работы студентов (Читальные залы библиотеки) | Компьютеры со свободным доступом в сеть Интернет и Электронным библиотечным и информационно-справочным системам | |
| Аудитория для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации | Комплекты мебели для учебного процесса – 30 шт., доска | |
| Аудитории для проведения занятий семинарского типа | Ауд. №332а: комп. класс каф. ИнфБ, количество ПЭВМ-12 (компьютер Cjrei54570, ауд.№ 420: комп. класс каф.ИнфБ, количество ПЭВМ - 12,(рабочая станция CPUCore 2DuoE6300 – 1.86), ауд. №424, комп класс каф. ИнфБ, количество ПЭВМ -12 (Компьютер Celeron D 2.8) | ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Веб-редактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc, Draw, Impress, Math, Writer. Персональная бухгалтерия HomeBank. Словарь Star Dict. iTest. VM Maxima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиаплеер Parole. Редактор тегов Easy TAG. Stath Studio. Pinta. Веб-браузер Mozilla Firefox. Графический редактор. FP – free Pascal. |

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

8.1 Оценочные материалы (ОМ) для дисциплины включают:

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 дисциплине определяются показатели и критерии оценивания сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

ОМ представляются отдельным комплектом и **входят в состав рабочей программы дисциплины.**

Оценочные материалы формируются в соответствии с П ВГУИТ «Положение об оценочных материалах».

Документ составлен в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем и специализации Безопасность открытых информационных систем.

**АННОТАЦИЯ
К РАБОЧЕЙ ПРОГРАММЕ
ДИСЦИПЛИНЫ
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
(наименование дисциплины)**

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6);
- способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);
- способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11).

В результате освоения дисциплины студент должен:

Знать

- цели, задачи, принципы и основные направления обеспечения информационной безопасности государства; основные термины по проблематике информационной безопасности; методологию создания систем защиты информации;
- перспективные направления развития средств и методов защиты информации, содержание информационной войны, методы и средства ее ведения.

Уметь

- выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;
- пользоваться современной научно-технической информацией по исследуемым проблемам и задачам.

Владеть

- навыками разработки политики информационной безопасности автоматизированных систем;
- навыками проектирования системы управления информационной безопасностью автоматизированной системы, навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем.

Содержание разделов дисциплины. Понятие информационной безопасности. Основные составляющие. Важность проблемы. Терминология и основные понятия защиты информации. Распространение объектно-ориентированного подхода на информационную безопасность. Законодательный уровень информационной безопасности. Мировые стандарты в области информационной безопасности. Российские стандарты в области информационной безопасности. Спецификации в области информационной безопасности. Особенности нормотворческой деятельности в области информационной безопасности. Угрозы информационной безопасности. Административный уровень информационной безопасности. Управление рисками. Процедурный уровень информационной безопасности. Основные программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация и управление доступом. Криптографические методы защиты информации.