МИНИСТЕРСТВО ВЫСШЕГО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»
Северо-Кавказский филиал

УТВЕРЖДАЮ:
Директор СКФ БГТУ
им. В.Г. Шухова
_____В.Л. Курбатов
«24» февраля 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.12 Организационная защита информации

Специальность

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация выпускника

Техник по защите информации

Форма обучения

очная

Срок обучения

3 года 10 месяцев

Минеральные Воды, 2021 г.

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта среднего профессионального образования (далее ФГОС СПО) по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного Приказом Министерства образования и науки РФ № 1553 от 09.12.2016 г.,
- Плана учебного процесса БГТУ им. В.Г. Шухова по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного в 2021 г.

Организация разработчик: СКФ ФГБОУ ВО «БГТУ им. В.Г. Шухова», Северо-Кавказский филиал

Составитель: к.э.н. _____ А.Н. Черниченко
ученая степень и звание подпись инициалы, фамилия

Рабочая программа обсуждена и рекомендована на заседании кафедры

Экономических и естественно-научных дисциплин
название кафедры

«_24_» _февраля_ 2021 г., протокол №_7__

Заведующий кафедрой: к.пед.н. _____ И.В. Черкасова
ученая степень и звание подпись инициалы, фамилия

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ 4

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ 6

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ 9

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ 11

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.12 «ОРГАНИЗАЦИОННАЯ ЗАЩИТА ИНФОРМАЦИИ»

1.1. Область применения программы

Рабочая программа учебной дисциплины входит в состав общепрофессионального цикла основной образовательной программы в соответствии с ФГОС СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем (квалификация «Техник по защите информации»).

1.2. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование у обучающихся самостоятельного, проблемного, творческого, критического мышления, стимулирование потребности к изучению компьютерных вирусов и информационной безопасности автоматизированных систем.

В результате изучения учебной дисциплины обучающийся должен:

уметь:

- использовать программные и аппаратные средства вычислительной техники для обеспечения безопасной работы персональных компьютеров, коммуникационных сетей и баз данных;
- осваивать и использовать антивирусные программы для защиты информации и вычислительных машин;
- осуществлять поиск новых знаний для решения профессиональных задач по борьбе с компьютерными вирусами;
- использовать программные методы и аппаратные средства для выявления и уничтожения компьютерных вирусов.

знать:

- условия возникновения, типы, структуру и особенности функционирования компьютерных вирусов;
- назначение и принципы работы распространенных антивирусных программ;
- алгоритмы поиска, блокировки и уничтожения компьютерных вирусов в персональных компьютерах, коммуникационных сетях и базах данных;
- стандартные процедуры восстановления поврежденной вирусами вычислительной техники и программного обеспечения;
- технические и программные средства борьбы с компьютерными вирусами.

1.3. Место дисциплины в структуре основной профессиональной образовательной

Учебная дисциплина ОП.12 «ОРГАНИЗАЦИОННАЯ ЗАЩИТА ИНФОРМАЦИИ» относится к общепрофессиональному циклу образовательной программы. До ее изучения обучающийся должен успешно освоить базовый курс дисциплины «Информатика».

Освоение данной дисциплины является необходимым условием для последующего изучения предусмотренных учебным планом дисциплин профессионального цикла. Изучается дисциплина обучающимися очной формы обучения **в 8 семестре**.

1.4. Планируемые результаты освоения дисциплины

В результате изучения дисциплины обучающийся должен освоить общие компетенции

Код	Общие компетенции
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 09.	Использовать информационные технологии в профессиональной деятельности

В результате освоения общих компетенций обучающийся должен

уметь	- распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника); - определять задачи поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска; - применять средства информационных технологий для решения профессиональных задач; использовать новое программное обеспечение;
знать	- актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте. алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности; - номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; - современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности;

В результате изучения дисциплины обучающийся должен освоить профессиональные компетенции

Код	**Профессиональные компетенции**
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами

В результате освоения профессиональных компетенций обучающийся должен

практический опыт	- установка, настройка программных средств защиты информации в автоматизированной системе; - обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использование программных и программно-аппаратных средств для защиты информации в сети.
умения	- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; - устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
	- особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в

знания	операционных системах, компьютерных сетях, базах данных; - особенности и способы применения программных и программно-аппаратных средств антивирусной защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных

1.5. Общее количество часов на освоение программы учебной дисциплины всего – 52 час, в том числе:
максимальной учебной нагрузки обучающегося **– 52 часов**, включая:
обязательной аудиторной учебной нагрузки обучающегося – **48** часов;
самостоятельной работы обучающегося – **4** часа.
По итогам обучения по программе учебной дисциплины ОП.12 «ОРГАНИЗАЦИОННАЯ ЗАЩИТА ИНФОРМАЦИИ» предусмотрен дифференцированный зачет **в 8 семестре**.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**
Максимальная учебная нагрузка (всего)	52
Обязательная аудиторная учебная нагрузка (всего)	48
в том числе:	-
лекции	28
практические занятия	-
лабораторные работы	20
Самостоятельная работа обучающегося (всего)	4
Форма промежуточной аттестации обучающегося (зачет/дифференцированный зачет/экзамен), семестр	диф. зачет 8 семестр

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов учебной дисциплины	Содержание учебного материала, практических занятий, самостоятельной учебной работы обучающихся	Объем часов	Уровень усвоения
1	2	3	4
	ОП.12 ОРГАНИЗАЦИОННАЯ ЗАЩИТА ИНФОРМАЦИИ	**52**	
Раздел 1. Введение в компьютерную вирусологию	**Содержание учебного материала**	**4**	
	Лекция №1. Объект, предмет, цель дисциплины и ее роль в системе знаний по информационной безопасности.	2	ознакомительный
	В том числе, лабораторные занятия	**2**	
	Лабораторное занятие №1. Обнаружение вирусной активности.	2	репродуктивный
Раздел 2. Происхождение компьютерных вирусов	**Содержание учебного материала**	**6**	
	Лекция №2 Понятие, условия создания и сущность компьютерных вирусов.	2	ознакомительный
	Лекция №3. Особенности структуры вирусных программ.	2	
	В том числе, лабораторные занятия	**2**	репродуктивный
	Лабораторное занятие №2. Изучение вирусной программы «почтовый червь».	2	
Раздел 3. Классификация компьютерных вирусов	**Содержание учебного материала**	**6**	
	Лекция №4. Виды компьютерных вирусов.	2	
	Лекция №5. Деструктивные действия вирусов на вычислительную технику.	2	
	В том числе, лабораторные занятия	**2**	ознакомительный
	Лабораторное занятие №3. Изучение вирусной «троянской» программы.	2	репродуктивный
Раздел 4. Распространение вирусных программ	**Содержание учебного материала**	**4**	
	Лекция №6. Каналы распространения и признаки проникновения вирусных программ в коммуникационные сети и вычислительные устройства.	2	ознакомительный
	В том числе, лабораторные занятия	**2**	
	Лабораторное занятие №4. Изучение макровируса.	2	репродуктивный
Раздел 5. Сетевые вирусные технологии	**Содержание учебного материала**	**4**	
	Лекция №7. Применение туннелинга, антитуннелинга и сокрытия как технологий функционирования в информационном пространстве.	2	
	В том числе, лабораторные занятия	**2**	
	Лабораторное занятие №5. Кодирование, полиморфизм и метаморфизм.	2	ознакомительный

1	2	3	4
Раздел 6. Методы обнаружения вирусов	**Содержание учебного материала**	**6**	ознакомительный
	Лекция №8. Возможность аппаратных и программных средств противодействовать распространению вирусов. Лекция №9. Методы обнаружения программ деструктивного воздействия.	2 2	
	В том числе, лабораторные занятия	**2**	репродуктивный
	Лабораторное занятие №6. Установка и работа антивирусного комплекса «Лаборатория Касперского».	2	
	Самостоятельная работа	**2**	продуктивный
	Создание презентаций по заданию «Методы обнаружения компьютерных вирусов».	2	
Раздел 7. Создание антивирусных программ	**Содержание учебного материала**	**8**	ознакомительный
	Лекция №10. Программные возможности блокировки функционирования вирусов. Лекция №11. Виды антивирусных программ.	2 2	
	В том числе, лабораторные занятия	**4**	репродуктивный
	Лабораторное занятие №7. Установка и работа антивирусной программы EsetNod32.	2	
	Лабораторное занятие №8. Установка и работа антивирусной программы DrWeb.	2	
Раздел 8. Формирование антивирусной защиты	**Содержание учебного материала**	**6**	ознакомительный
	Лекция №12. Задачи противодействия вирусам и выбор антивирусной программы. Лекция №13. Характеристики и применение отечественных антивирусных разработок.	2 2	
	В том числе, лабораторные занятия	**2**	репродуктивный
	Лабораторное занятие №9. Разработка антивирусной программы «ревизор».	2	
	Самостоятельная работа	**2**	продуктивный
	Подготовка доклада «Оценка защищенности сетей от компьютерных вирусов»	2	
Раздел 9. Системы антивирусной защиты	**Содержание учебного материала**	**4**	ознакомительный
	Лекция №14. Разработка комплексной антивирусной системы защиты. Лекция №15. Организация защиты корпоративной сети от вредоносных программ.	1 1	
	В том числе, лабораторные занятия	**2**	репродуктивный
	Лабораторное занятие №10. Выбор антивирусного комплекса методом функциональной полноты.	2	
Промежуточная аттестация по учебной дисциплине (дифференцированный зачет)		**-**	
Всего:		**52**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Наименование учебных помещений и помещений для самостоятельной работы

Наименование учебных помещений* и помещений для самостоятельной работы	Оснащенность учебных помещений и помещений для самостоятельной работы	Перечень лицензионного и свободно распространяемого программного обеспечения. Реквизиты подтверждающего документа
Кабинет информационной безопасности. № 20. Лаборатория технических средств защиты информации. Для проведения лекций, практических занятий, консультаций, текущих и промежуточных аттестаций. Оснащен информационными стендами, по 10 компьютеров на базе процессора Dual Core Intel Core i3, оперативной памятью 4ГБ и жестким диском 500 ГБ, локальной сетью с пропускной способностью 100 Мбит/с, операционная система Windows 7 (32-bit).	Оснащение: - рабочее место преподавателя: один стол и один стул; - посадочные места по количеству обучающихся: 1 стул на одного ученика и один стол на два человека; - комплекты учебно-методических и наглядных пособий. Оборудование: - ПК, экран, проектор, колонки, учебная доска.	1. Операционная система Windows7 (License №64080343 от 15.09.2014 г.) 2. Офисный пакет приложений Microsoft Office 2007 (License №43846774 от 25.02.2008 г.) 3. Антивирусные программы: - Антивирус Касперского; - EsetNod32; - DrWeb.

3.2. Информационное обеспечение обучения: перечень рекомендуемых учебных изданий, интернет-ресурсов, дополнительной литературы, периодических изданий, программного обеспечения

3.2.1. Основная литература

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум / под редакцией А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469235.
2. Аверченков, В. И. Организационная защита информации : учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов. — Брянск : Брянский государственный технический университет, 2012. — 184 с. — ISBN 978-89838-489-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/7002.html. — Режим доступа: для авторизир. пользователей

3.2.2. Дополнительная литература

1. Рагозин, Ю. Н. Инженерно-техническая защита информации : учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности / Ю. Н. Рагозин ; под редакцией Т. С. Кулакова. — Санкт-Петербург : Интермедия, 2018. — 168 с. — ISBN 978-5-4383-0161-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/73641.html. — Режим доступа: для авторизир. пользователей

3.2.3 Официальные, справочно-библиографические и периодические издания

1. Российская Федерация. Законы. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (изменениями, одобренными в ходе общероссийского голосовании 1 июля 2020 года : одобрен Государственной Думой 11 марта 2020 года : одобрен Советом Федерации 11 марта 2020 года // СПС КонсультантПлюс // Режим доступа : для зарегистрированных пользователей.
2. Российская Федерация. Законы. Об образовании в Российской Федерации : принят Государственной Думой 21 декабря 2012 года : одобрен Советом Федерации 26 декабря 2012 года // СПС КонсультантПлюс // Режим доступа: для зарегистрированных пользователей.
3. Российская Федерация. Законы. Трудовой кодекс Российской Федерации : принят Государственной Думой 21 декабря 2001 года : одобрен Советом Федерации 26 декабря 2001 года (с изменениями принятыми ФЗ от 25.05.2020 № 157-ФЗ : принят Государственной Думой 13 мая 2020 года : одобрен Советом Федерации 20 мая 2020 года // СПС КонсультантПлюс: Режим доступа: для зарегистрированных пользователей.
4. Федеральные государственные образовательные стандарты среднего профессионального образования // Доступ к СПС КонсультантПлюс.
5. Компьютерные энциклопедии, справочники, глоссарии: энциклопедические справочники и словари по информационным технологиям – http://www.garshin.ru/it/it-terms.html

3.2.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), необходимых для освоения дисциплины

1. Непрерывное информационное образование: проект издательства «БИНОМ. Лаборатория знаний» http://www.metodist.lbz.ru
2. www.edu/ru/modules.php - каталог образовательных Интернет-ресурсов: учебно-методические пособия
3. http://www.phis.org.ru/informatica/ - сайт Информатика
4. http://www.km.ru/ - энциклопедия
5. http://www.ege.ru/ - тесты по информационной безопасности
6. http://comp-science.narod.ru/ - дидактические материалы по информационной безопасности.

3.2.5. Перечень программного обеспечения, профессиональных баз данных и информационных справочных систем

Программное обеспечение.

1. Операционная система Windows 7 (License № 64080343 от 15.09.2014);
2.Офисный пакет приложений Microsoft Office 2007 (License № 43846774 от 25.02.2008).

Профессиональные базы данных и информационные справочные системы.

1. ИС «Техэксперт». Режим доступа из корпоративной сети университета: http://sk5-410-libte.at.urfu.ru/docs/
2. Портал информационно-образовательных ресурсов (http://study.ustu.ru)
3. Поисковые системы: Google (http://google.ru), Yandex (http://yandex.ru).
5. База нормативной технической документации (http://www.complexdoc.ru).
6. Поисковая система (http://www.freepatent.ru/).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения тестирования, а также выполнения обучающимися индивидуальных заданий и исследований.

Результаты обучения (освоенные умения, усвоенные знания) **Результатом освоения учебной дисциплины являются следующие**	**Основные показатели оценки результата**	**Формы и методы контроля**
умения: – использовать программные и аппаратные средства вычислительной техники для обеспечения безопасной работы персональных компьютеров, коммуникационных сетей и баз данных;	Выполнение практических работ в соответствии с заданием	Оценка результатов выпол- - нения практических работ. Экспертное наблюдение за выполнением работ.
– осваивать и использовать антивирусные программы для защиты информации и вычислительных машин;	Выполнение практических работ в соответствии с заданием	Оценка результатов выполнения прикладных задач.Экспертное наблюдение за выполнением работ.
– осуществлять поиск новых знаний для решения профессиональных задач по борьбе с компьютерными вирусами;	Выполнение практических работ в соответствии с заданием	Оценка результатов поиска информации. Экспертное наблюдение за выполнением работ.
– использовать програм - мные методы и аппаратные средства для выявления и уничтожения компьютерных вирусов.	Демонстрация умения составлять программы в соответствии с заданием	Оценка результатов составления программ. Защита выполненной работы.
знания: - условия возникновения, типы, структуру и особенности функционирования компьютерных вирусов;	Демонстрация знаний вычислительной техники при выполнении индивидуальных заданий	Оценка устных ответов обучающихся при работе с компьютером.
– назначение и принципы работы распространенных антивирусных программ;	Демонстрация знаний вычи слительной техники при вы полнении заданий	Оценка устных ответов на контрольные вопросы.
– алгоритмы поиска, блокировки и уничтожения компьютерных ви - русов в персональных компьютерах, коммуникационных сетях и базах данных;	Демонстрация знаний вычислительной техники при выполнении индивидуальных заданий	Оценка письменных ответов на контрольные вопросы.
- стандартные процедуры восста - новления поврежденной вирусами вычислительной техники и программного обеспечения;	Демонстрация знаний по типам данных при выполне -нии письменных заданий	Оценка письменных ответов на контрольные вопросы.
– технические и програм- мные средства борьбы с компьютерными вирусами.	Демонстрация знаний по работе офисных программ при индивидуальных опросах	Оценка устных ответов на контрольные вопросы.