МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГТУ», ВГТУ)

ЦЕНТР ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

Утверждаю:

Проректор по учебной работе

_____ Полосов А.И.
(Подпись) *(И.О. Фамилия)*

«____» _____ 2024 г.
(дата)

ПРОГРАММА ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

Информационная безопасность
(наименование программы)

_____
(наименование присваиваемой квалификации (при наличии))

СОГЛАСОВАНО:

Директор ЦДПО _____ Р.А. Шепс
(подпись) *(И.О. Фамилия)*

Автор программы _____ Е.А. Тарасов
(подпись) *(И.О. Фамилия)*

Воронеж- 2024

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель и задачи реализации программы

формирование у обучающихся принципов информационной безопасности государства, подходов к анализу его информационной инфраструктуры, принципов организации, проектирования и анализа систем защиты информации, освоения основ их комплексного построения на различных уровнях защиты и особенностей степеней защиты для государственного и частного назначения.

1.2. Характеристика нового вида профессиональной деятельности, новой квалификации

а) Область профессиональной деятельности:
– Образование и наука (в сфере научных исследований);
– Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере);
– Обеспечение безопасности (в сфере эксплуатации технических и программно- аппаратных средств защиты информации).
б) Объекты профессиональной деятельности выпускников, освоивших программу:
– прикладные и информационные процессы;
– информационные системы;
– информационные технологии.
– информационные процессы, технологии, системы и сети, их инструментальное (программное, техническое, организационное) обеспечение, способы и методы проектирования, отладки, производства и эксплуатации информационных технологий и систем в различных областях и сферах цифровой экономики;
– программное обеспечение (общего и прикладного характера), способы и методы проектирования, разработки, отладки, оценки качества, проверки работоспособности и модификации программного обеспечения;
– информационные системы, базы данных, способы и методы поддержки эффективной работы баз данных;
– техническая документация информационно-методического и маркетингового назначения в сфере информационных технологий;
– информационные процессы, технологии, системы и сети, их инструментальное (программное, техническое, организационное) обеспечение, способы и методы проектирования, отладки, производства и эксплуатации информационных технологий и систем в различных областях и сферах цифровой экономики;
– проекты в области информационных технологий.

Нормативные документы для разработки ППП:
Приказ Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427 «Об утверждении федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность»;
Приказ Минтруда России от 12.04.2013 № 148н «Об утверждении уровней квалификации в целях разработки проектов профессиональных стандартов».

Приказ Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 533н «Об утверждении профессионального стандарта «Специалист по безопасности компьютерных систем и сетей»».
Приказ Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах»».
Приказ Министерства труда и социальной защиты Российской Федерации от 09.89.2022 № 474н «Об утверждении профессионального стандарта «Специалист по технической защите информации»».
Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
Приказ Минобрнауки России от 5 апреля 2017 г. № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры»;
Федеральный закон от 02.12.2019 г. №403-ФЗ «О внесении изменений в Федеральный закон «Об образовании в Российской Федерации» и отдельные законодательные акты Российской Федерации»;
Устав ВГТУ;
Локальные нормативные акты и методические документы ВГТУ

1.3 Требования к результатам освоения программы

В соответствии с выбранными трудовыми функциями и с учетом необходимого квалификационного уровня ППП устанавливает следующие профессиональные компетенции и планируемые результаты освоения программы:

Тип задач профессиональной деятельности	Код и наименование профессиональной компетенции	Планируемые результаты обучения по дисциплинам
производственно-технологический	**ПК-1** Способность использовать нормативные правовые акты, методические документы, международные и национальные стандарты в области защиты информации в своей профессиональной деятельности	Знать: типовые структуры управления, связи и автоматизации объектов информатизации, требования к их оснащенности техническими средствами; порядок проведения аттестации объектов информатизации по требованиям безопасности информации; организацию и содержание проведения работ по ТЗКИ, состав и содержание необходимых документов (в том числе по защите информации от утечки по техническим каналам, по защите информации от несанкционированного доступа (НСД) и по защите информации от специальных воздействий); Уметь: работать с действующей нормативной правовой и методической базой в области защиты информации; определять возможные ТКУИ и угрозы

		безопасности информации в результате НСД и специальных воздействий; определять требования к программным и аппаратным средствам, предназначенным для хранения, обработки и передачи информации; разрабатывать проекты документов (положений, инструкций, руководств и др.) в области ТЗКИ, а также оформлять результаты аттестации объектов информатизации по требованиям безопасности информации; Владеть: проведения организационных и технических мероприятий по ТЗКИ, контроля защищенности информации; работы с современными операционными системами; установки и настройки современных операционных систем с учетом требований по безопасности информации; установки и настройки современных средств защиты информации, системного и прикладного программного обеспечения с учетом требований по безопасности информации; разработки, документирования баз данных, компьютерных сетей с учетом требований по безопасности информации
производственно-технологический	**ПК-2** Способность использовать достижения науки и техники в области защиты информации, пользоваться реферативными и справочно-информационными изданиями в области защиты информации	Знать: действующую систему сертификации средств защиты информации по требованиям безопасности информации; основы лицензирования деятельности по ТЗКИ и (или) деятельности по разработке и производству средств защиты конфиденциальной информации; физические основы возникновения, классификацию и характеристики ТКУИ; угрозы безопасности информации; цели, задачи, основы организации, основные способы и средства ТЗКИ и контроля защищенности информации Уметь: разрабатывать технические задания на проведение научно-исследовательских и опытно-конструкторских работ в области ТЗКИ; проводить работы по классификации защищенности автоматизированных систем от НСД к информации, аттестации объектов информатизации; применять подсистемы разграничения доступа, подсистемы обнаружения атак, методы анализа результатов проверок, учета нарушений

		требований по ТЗКИ Владеть: определения задач, способов и средств ТЗКИ и контроля защищенности информации; использования программных и аппаратных средств ТЗКИ и контроля защищенности информации; проведения организационных и технических мероприятий по ТЗКИ, контроля защищенности информации; работы с современными операционными системами; установки и настройки современных операционных систем с учетом требований по безопасности информации
производственно-технологический	**ПК-3** Способность определять возможные ТКУИ и угрозы безопасности информации на основе анализа информационных процессов в организации, целей и задач деятельности объекта защиты	Знать: нормативные правовые акты, методические документы, международные и национальные стандарты в области защиты информации; основы построения информационных систем и формирования информационных ресурсов; виды конфиденциальной информации; перечни сведений конфиденциального характера, основные требования и рекомендации по их защите Уметь: осуществлять аутентификацию взаимодействующих объектов, проверку подлинности отправителя и целостности передаваемых данных; применять штатные средства ТЗКИ и контроля защищенности информации, осуществлять контроль защищенности информации; устанавливать, монтировать, устранять неисправности оборудования для обеспечения ТЗКИ, контролировать оснащенность объекта защиты; проводить организационные и технические мероприятия по ТЗКИ Владеть: организации деятельности подразделений и специалистов в области ТЗКИ в органах государственной власти и организациях; работы с действующей нормативной правовой и методической базой в области защиты информации; разработки необходимой документации по вопросам организации ТЗКИ в органах государственной власти и организациях; выявления ТКУИ и

		определения угроз безопасности информации применительно к конкретным объектам защиты

1.4. Требования к уровню подготовки поступающего на обучение, необходимому для освоения программы

Обучение по данной программе будет проходить у лиц, которые имеют высшее, средне профессиональной образование или является студентом последнего курса обучения.

1.5. Трудоемкость обучения - _____256 часов_____

(количество часов или зачетных единиц)

1.6. Форма обучения

- очно-заочная с применением дистанционных образовательных технологий/заочная с применением дистанционных образовательных технологий.

Освоение программы осуществляется без отрыва от работы.

Форма обучения устанавливается при наборе группы слушателей.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГТУ», ВГТУ)

ЦЕНТР ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

Утверждаю:

Проректор по учебной работе

_____ А. И. Колосов
(подпись) *(И.О. Фамилия)*

«_____» _____ 2024 г.

УЧЕБНЫЙ ПЛАН

Информационная безопасность

(наименование присваиваемой квалификации (при наличии))

СОГЛАСОВАНО:

Директор ЦДПО _____ Р.А. Шепс
(подпись) *(И.О. Фамилия)*

Автор программы _____ Е.А. Тарасов

УЧЕБНЫЙ ПЛАН
«Информационная безопасность»

Цель: формирование у обучающихся принципов информационной безопасности государства, подходов к анализу его информационной инфраструктуры, принципов организации, проектирования и анализа систем защиты информации, освоения основ их комплексного построения на различных уровнях защиты и особенностей степеней защиты для государственного и частного назначения.

Категория: Слушатели имеющие высшее, средне профессиональной образование или являются студентами последнего курса обучения.
Срок обучения: 256 часов
Режим занятий: 8 часов в день, 2 месяцев
Форма обучения: очно-заочная с применением дистанционных образовательных технологий.
Уровень образования: высшее, средне профессиональное

Наименование дисциплины	Общая трудоемкость	Число часов аудиторных занятий				Внеаудиторная работа	
		ЛК	К	Зачет	Экзамен	СР	АР
Основные понятия теории информационной безопасности Информация как объект защиты Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	22	15	5	2			-
Угрозы информационной безопасности Построение систем защиты от угрозы нарушения конфиденциальности Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	16	10	4	2			-
Политика и модели безопасности Обзор международных стандартов информационной безопасности Информационные войны и информационное противоборство	22	20		2			-
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	24	18	4	2			-

Наименование дисциплины	Общая трудоемкость	Число часов аудиторных занятий				Внеаудиторная работа	
		ЛК	К	Зачет	Экзамен	СР	АР
БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ. ТРАДИЦИОННЫЙ ПОДХОД К АНАЛИЗУ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТНО-ОРИЕНТИРОВАННЫЙ ПОДХОД – ПЕРСПЕКТИВНЫЙ ПРИНЦИП АНАЛИЗА ВОПРОСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ							
ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И КРИТЕРИИ КЛАССИФИКАЦИИ УГРОЗ УРОВНИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	31	25	4	2			-
АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕДУРНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОСНОВНЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	37	25	10	2			-
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ ВРЕДОНОСТНЫЕ ПРОГРАММЫ	32	30		2			-
ОСНОВЫ БОРЬБЫ С ВРЕДОНОСТНЫМИ ПРОГРАММАМИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГЛОБАЛЬНЫХ СЕТЯХ	16	12	2	2			-

Наименование дисциплины	Общая трудоемкость	Число часов аудиторных занятий				Внеаудиторная работа	
		ЛК	К	Зачет	Экзамен	СР	АР
МЕХАНИЗМЫ РЕАЛИЗАЦИИ УДАЛЕННЫХ АТАК В ГЛОБАЛЬНОЙ СЕТИ INTERNET							
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМ ВХОДЯЩИХ В СОСТАВ ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ ОБЕСПЕЧЕНИЕ БЕЗОПАСТНОГО ВЗАИМОДЕЙСТВИЯ В ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОПЕРАЦИОННЫХ СИСТЕМАХ И ПРОГРАММНОМ ОБЕСПЕЧЕНИИ	32	30		2			-
ОСНОВЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА UNIX БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	22	15	5	2			-
Итоговая аттестация	2				2		-
ИТОГО:	**256**	**221**	**29**	**20**	**2**		

Примечания:
При организации учебного процесса частично реализуются дистанционные образовательные технологии.
Итоговая аттестация включает экзамен в форме тестирования.
Принятые сокращения: ЛК – лекции, К – консультация, СР – самостоятельная работа, АР – аттестационная работа.

Срок обучения: 256 часов
Режим занятий: 8 часов в день, 2 месяцев
Форма обучения: заочная с применением дистанционных образовательных технологий.
Форма организации учебного процесса: модульная
Уровень образования: высшее, средне профессиональное
Общая трудоемкость: 28 зачетные единицы, 256 часов, в том числе с применением дистанционных технологий 256 часов

Наименование дисциплины	**Общая трудоемкость**	**С применением дистанционных технологий**			
		Консультации[1]	**Промежуточная аттестация[2]**	**Итоговая аттестация[3]**	**Самостоятельная работа[4]**
Основные понятия теории информационной безопасности Информация как объект защиты Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	22	1	1		20
Угрозы информационной безопасности Построение систем защиты от угрозы нарушения конфиденциальности Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	16	1	1		14
Политика и модели безопасности Обзор международных стандартов информационной безопасности Информационные войны и информационное противоборство	22	1	1		20
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ.	24	1	1		22

Наименование дисциплины	Общая трудоемкость	С применением дистанционных технологий			
		Консультации[1]	Промежуточная аттестация[2]	Итоговая аттестация[3]	Самостоятельная работа[4]
ТРАДИЦИОННЫЙ ПОДХОД К АНАЛИЗУ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТНО-ОРИЕНТИРОВАННЫЙ ПОДХОД – ПЕРСПЕКТИВНЫЙ ПРИНЦИП АНАЛИЗА ВОПРОСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ					
ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И КРИТЕРИИ КЛАССИФИКАЦИИ УГРОЗ УРОВНИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	31	1	1		29
АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕДУРНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОСНОВНЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	37	1	1		35
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ ВРЕДОНОСТНЫЕ ПРОГРАММЫ	32	1	1		30
ОСНОВЫ БОРЬБЫ С ВРЕДОНОСТНЫМИ	16	1	1		14

Наименование дисциплины	Общая трудоемкость	С применением дистанционных технологий			
		Консультации[1]	Промежуточная аттестация[2]	Итоговая аттестация[3]	Самостоятельная работа[4]
ПРОГРАММАМИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГЛОБАЛЬНЫХ СЕТЯХ МЕХАНИЗМЫ РЕАЛИЗАЦИИ УДАЛЕННЫХ АТАК В ГЛОБАЛЬНОЙ СЕТИ INTERNET					
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМ ВХОДЯЩИХ В СОСТАВ ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ ОБЕСПЕЧЕНИЕ БЕЗОПАСТНОГО ВЗАИМОДЕЙСТВИЯ В ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОПЕРАЦИОННЫХ СИСТЕМАХ И ПРОГРАММНОМ ОБЕСПЕЧЕНИИ	32	1	1		30
ОСНОВЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА UNIX БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	22	1	1		20
Итоговая аттестация	2			2	
ИТОГО:	**256**	**10**	**10**	**2**	**234**

[1] Консультация проводится в формате видеоконференции.
Дата и время проведения видеоконференции согласовываются между слушателем и руководителем программы
[2]Промежуточная аттестация проводится в виде зачета в форме устного ответа в формате видео конференции.
Дата и время проведения видеоконференции согласовываются между слушателем и руководителем программы
[3] Итоговая аттестация проводится в форме тестирования применением ЭИОС ВГТУ
[4] Самостоятельная работа осуществляется слушателем с использование материалов из ЭИОС ВГТУ. График /расписание самостоятельной работы не устанавливается

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГТУ», ВГТУ)

ЦЕНТР ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

Утверждаю:

Проректор по учебной работе

_____ А.И. Колосов
(подпись) *(И.О. Фамилия)*

«___» _____ 2024 г.

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

Дополнительная профессиональная программа
(профессиональная переподготовка)

Информационная безопасность

(наименование присваиваемой квалификации (при наличии))

СОГЛАСОВАНО:

Директор ЦДПО _____ Р.А. Шепс
(подпись) *(И.О. Фамилия)*

Автор программы _____ Е.А. Тарасов

УЧЕБНО – ТЕМАТИЧЕСКИЙ ПЛАН

Дополнительная профессиональная программа

(профессиональная переподготовка)

«Информационная безопасность»

Цель: формирование у обучающихся принципов информационной безопасности государства, подходов к анализу его информационной инфраструктуры, принципов организации, проектирования и анализа систем защиты информации, освоения основ их комплексного построения на различных уровнях защиты и особенностей степеней защиты для государственного и частного назначения.

Категория: Слушатели имеющие высшее, средне профессиональной образование или являются студентами последнего курса обучения.
Срок обучения: 256 часов
Режим занятий: 8 часов в день, 2 месяцев
Форма обучения: очно-заочная с применением дистанционных образовательных технологий.
Уровень образования: высшее, средне профессиональное

Наименование дисциплины	Общая трудоемкость	Число часов аудиторных занятий				Внеаудиторная работа	
		ЛК	К	Зачет	Экзамен	СР	АР
Основные понятия теории информационной безопасности Информация как объект защиты Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	22	15	5	2			-
Угрозы информационной безопасности Построение систем защиты от угрозы нарушения конфиденциальности Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	16	10	4	2			-
Политика и модели безопасности Обзор международных стандартов информационной безопасности Информационные войны и информационное противоборство	22	20		2			-
ОСНОВЫ ИНФОРМАЦИОННОЙ	24	18	4	2			-

Наименование дисциплины	Общая трудоемкость	Число часов аудиторных занятий				Внеаудиторная работа	
		ЛК	К	Зачет	Экзамен	СР	АР
БЕЗОПАСНОСТИ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ. ТРАДИЦИОННЫЙ ПОДХОД К АНАЛИЗУ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТНО-ОРИЕНТИРОВАННЫЙ ПОДХОД – ПЕРСПЕКТИВНЫЙ ПРИНЦИП АНАЛИЗА ВОПРОСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ							
ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И КРИТЕРИИ КЛАССИФИКАЦИИ УГРОЗ УРОВНИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	31	25	4	2			-
АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕДУРНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОСНОВНЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	37	25	10	2			-
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ ВРЕДОНОСТНЫЕ ПРОГРАММЫ	32	30		2			-
ОСНОВЫ БОРЬБЫ С ВРЕДОНОСТНЫМИ ПРОГРАММАМИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В	16	12	2	2			-

Наименование дисциплины	Общая трудоемкость	Число часов аудиторных занятий				Внеаудиторная работа	
		ЛК	К	Зачет	Экзамен	СР	АР
ГЛОБАЛЬНЫХ СЕТЯХ МЕХАНИЗМЫ РЕАЛИЗАЦИИ УДАЛЕННЫХ АТАК В ГЛОБАЛЬНОЙ СЕТИ INTERNET							
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМ ВХОДЯЩИХ В СОСТАВ ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ ОБЕСПЕЧЕНИЕ БЕЗОПАСТНОГО ВЗАИМОДЕЙСТВИЯ В ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОПЕРАЦИОННЫХ СИСТЕМАХ И ПРОГРАММНОМ ОБЕСПЕЧЕНИИ	32	30		2			-
ОСНОВЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА UNIX БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	22	15	5	2			-
Итоговая аттестация	2				2		-
ИТОГО:	**256**	**221**	**29**	**20**	**2**		

Примечания:

При организации учебного процесса частично реализуются дистанционные образовательные технологии.

Итоговая аттестация включает экзамен в форме тестирования.

Принятые сокращения: ЛК – лекции, К – консультация, СР – самостоятельная работа, АР – аттестационная работа.

Срок обучения: 256 часов
Режим занятий: 8 часов в день, 2 месяцев
Форма обучения: заочная с применением дистанционных образовательных технологий.
Форма организации учебного процесса: модульная
Уровень образования: высшее, средне профессиональное
Общая трудоемкость: 28 зачетные единицы, 256 часов, в том числе с применением дистанционных технологий 256 часов

Наименование дисциплины	**Общая трудоемкость**	**С применением дистанционных технологий**			
		Консультации[1]	**Промежуточная аттестация[2]**	**Итоговая аттестация[3]**	**Самостоятельная работа[4]**
Основные понятия теории информационной безопасности Информация как объект защиты Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	22	1	1		20
Угрозы информационной безопасности Построение систем защиты от угрозы нарушения конфиденциальности Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	16	1	1		14
Политика и модели безопасности Обзор международных стандартов информационной безопасности Информационные войны и информационное противоборство	22	1	1		20
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ.	24	1	1		22

Наименование дисциплины	Общая трудоемкость	С применением дистанционных технологий			
		Консультации[1]	Промежуточная аттестация[2]	Итоговая аттестация[3]	Самостоятельная работа[4]
ТРАДИЦИОННЫЙ ПОДХОД К АНАЛИЗУ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТНО-ОРИЕНТИРОВАННЫЙ ПОДХОД – ПЕРСПЕКТИВНЫЙ ПРИНЦИП АНАЛИЗА ВОПРОСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ					
ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И КРИТЕРИИ КЛАССИФИКАЦИИ УГРОЗ УРОВНИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	31	1	1		29
АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕДУРНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОСНОВНЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	37	1	1		35
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ ВРЕДОНОСТНЫЕ ПРОГРАММЫ	32	1	1		30
ОСНОВЫ БОРЬБЫ С ВРЕДОНОСТНЫМИ	16	1	1		14

Наименование дисциплины	Общая трудоемкость	С применением дистанционных технологий			
		Консультации[1]	Промежуточная аттестация[2]	Итоговая аттестация[3]	Самостоятельная работа[4]
ПРОГРАММАМИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГЛОБАЛЬНЫХ СЕТЯХ МЕХАНИЗМЫ РЕАЛИЗАЦИИ УДАЛЕННЫХ АТАК В ГЛОБАЛЬНОЙ СЕТИ INTERNET					
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМ ВХОДЯЩИХ В СОСТАВ ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ ОБЕСПЕЧЕНИЕ БЕЗОПАСТНОГО ВЗАИМОДЕЙСТВИЯ В ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОПЕРАЦИОННЫХ СИСТЕМАХ И ПРОГРАММНОМ ОБЕСПЕЧЕНИИ	32	1	1		30
ОСНОВЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА UNIX БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	22	1	1		20
Итоговая аттестация	2			2	
ИТОГО:	**256**	**10**	**10**	**2**	**234**

[1] Консультация проводится в формате видеоконференции.
Дата и время проведения видеоконференции согласовываются между слушателем и руководителем программы
[2]Промежуточная аттестация проводится в виде зачета в форме устного ответа в формате видео конференции.
Дата и время проведения видеоконференции согласовываются между слушателем и руководителем программы
[3] Итоговая аттестация проводится в форме тестирования применением ЭИОС ВГТУ
[4] Самостоятельная работа осуществляется слушателем с использование материалов из ЭИОС ВГТУ. График /расписание самостоятельной работы не устанавливается

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГТУ», ВГТУ)

ЦЕНТР ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

График

проведения занятий по программе профессиональной переподготовки:

«Информационная безопасность»
(наименование программы)
256 часов

СОГЛАСОВАНО:

Директор ЦДПО _____ Р. А. Шепс
(подпись) *(И.О. Фамилия)*

Расписание учебных занятий

1 месяц					2 месяц				
1/НО	8/УЗ	15/УЗ	22/УЗ	29/УЗ		6/УЗ	13/УЗ	20/УЗ	27/УЗ
2/УЗ	9/УЗ	16/УЗ	23/УЗ	30/УЗ		7/УЗ	14/УЗ	21/УЗ	28/УЗ
3/УЗ	10/УЗ	17/УЗ	24/УЗ		1/УЗ	8/УЗ	15/УЗ	22/УЗ	29/УЗ
4/УЗ	11/УЗ	18/УЗ	25/УЗ		2/УЗ	9/УЗ	16/УЗ	23/УЗ	30/УЗ
5/УЗ	12/УЗ	19/КО	26/УЗ		3/УЗ	10/УЗ	17/УЗ	24/УЗ	31 /КО

Условные обозначения:
НО/КО - начало обучения / конец обучения;
УЗ - учебные занятия;
ИА - итоговая аттестация.

4 Организационно-педагогические условия реализации программы

4.1. Материально-технические условия реализации программы

Наименование специализированных аудиторий, кабинетов, лабораторий (с указанием адреса)	**Вид занятий**	**Наименование оборудования, программного обеспечения**
1	**2**	**3**
Аудитория	лекции	Аудитория, оснащённая мультимедийным оборудованием (проектор, экран, звуковоспроизводящее оборудование), обеспечивающим демонстрацию (воспроизведение) мультимедиа-материалов. https://profedu.cchgeu.ru/

4.2. Учебно-методическое обеспечение программы

Используемые в учебном процессе учебные пособия, изданные по отдельным разделам программы; профильная литература; отраслевые и другие и другие нормативные документы; электронные ресурсы.

4.3. Кадровое обеспечение дисциплины

В реализации учебного процесса по **«Информационная безопасность»** участвуют следующие преподаватели и сотрудники:

Фамилия, имя, отчество, должность по штатному расписанию	Какое образовательное учреждение окончил, специальность (направление подготовки) по документу об образовании	Ученая степень, ученое (почетное) звание, квалификационная категория	Стаж работы			Основное место работы, должность	Условия привлечения к педагогической деятельности (штатный работник, внутренний совместитель, внешний совместитель, иное)
			Всего	в т.ч. педагогической работы			
				Всего	в т.ч. по указанной дисциплине		
1	2	3	4	5	6	7	8
Тарасов Евгений Александрович	ВО по специальности «Автомобили и автомобильное хозяйство», квалификация Инженер по специальности Автомобили и автомобильное хозяйство	Доцент К.т.н.	17	17	17	ФГБОУ ВО «ВГТУ»	штатный

5. Формы аттестации
Оценка качества освоения программы включает итоговую аттестацию обучающихся.

6. Особенности освоения программ ДПО для обучающихся с ограниченными возможностями здоровья

Реализация программы для лиц с ОВЗ реализуется на основание статьи 79 Федерального закон от 29.12.2012 N 273-ФЗ (ред. от 30.12.2021) "Об образовании в Российской Федерации" а также другими действующими нормативными актами.

7. Выдаваемый документ об образовании.
В соответствии с п. 19 Порядка осуществления деятельности по программам ДПО (Приказ Минобрнауки России №499 от 01.07.2013 г.) после освоения программ подготовки выдаются либо диплом о переподготовке, либо удостоверение о повышении квалификации установленного образца.

РАБОЧАЯ ПРОГРАММА
дисциплины (модуля)

«Информационная безопасность»

наименование дисциплины (модуля) в соответствии с учебным планом)

Цели и задачи дисциплины

формирование у обучающихся принципов информационной безопасности государства, подходов к анализу его информационной инфраструктуры, принципов организации, проектирования и анализа систем защиты информации, освоения основ их комплексного построения на различных уровнях защиты и особенностей степеней защиты для государственного и частного назначения.

ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения направлен на формирование следующих компетенций:

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**
ПК-1 Способность использовать нормативные правовые акты, методические документы, международные и национальные стандарты в области защиты информации в своей профессиональной деятельности	Знать: типовые структуры управления, связи и автоматизации объектов информатизации, требования к их оснащенности техническими средствами; порядок проведения аттестации объектов информатизации по требованиям безопасности информации; организацию и содержание проведения работ по ТЗКИ, состав и содержание необходимых документов (в том числе по защите информации от утечки по техническим каналам, по защите информации от несанкционированного доступа (НСД) и по защите информации от специальных воздействий); Уметь: работать с действующей нормативной правовой и методической базой в области защиты информации; определять возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий; определять требования к программным и аппаратным средствам, предназначенным для хранения, обработки и передачи информации; разрабатывать проекты документов (положений, инструкций, руководств и др.) в области ТЗКИ, а также оформлять результаты аттестации объектов информатизации по требованиям безопасности информации; Владеть: проведения организационных и технических мероприятий по ТЗКИ, контроля защищенности информации; работы с современными операционными системами; установки и настройки современных операционных систем с учетом требований по безопасности информации; установки и настройки современных средств защиты информации, системного и прикладного программного обеспечения с учетом требований по безопасности информации; разработки, документирования баз данных, компьютерных сетей с учетом требований по безопасности информации

ПК-2 Способность использовать достижения науки и техники в области защиты информации, пользоваться реферативными и справочно-информационными изданиями в области защиты информации	Знать: действующую систему сертификации средств защиты информации по требованиям безопасности информации; основы лицензирования деятельности по ТЗКИ и (или) деятельности по разработке и производству средств защиты конфиденциальной информации; физические основы возникновения, классификацию и характеристики ТКУИ; угрозы безопасности информации; цели, задачи, основы организации, основные способы и средства ТЗКИ и контроля защищенности информации Уметь: разрабатывать технические задания на проведение научно-исследовательских и опытно-конструкторских работ в области ТЗКИ; проводить работы по классификации защищенности автоматизированных систем от НСД к информации, аттестации объектов информатизации; применять подсистемы разграничения доступа, подсистемы обнаружения атак, методы анализа результатов проверок, учета нарушений требований по ТЗКИ Владеть: определения задач, способов и средств ТЗКИ и контроля защищенности информации; использования программных и аппаратных средств ТЗКИ и контроля защищенности информации; проведения организационных и технических мероприятий по ТЗКИ, контроля защищенности информации; работы с современными операционными системами; установки и настройки современных операционных систем с учетом требований по безопасности информации
ПК-3 Способность определять возможные ТКУИ и угрозы безопасности информации на основе анализа информационных процессов в организации, целей и задач деятельности объекта защиты	Знать: нормативные правовые акты, методические документы, международные и национальные стандарты в области защиты информации; основы построения информационных систем и формирования информационных ресурсов; виды конфиденциальной информации; перечни сведений конфиденциального характера, основные требования и рекомендации по их защите Уметь: осуществлять аутентификацию взаимодействующих объектов, проверку подлинности отправителя и целостности передаваемых данных; применять штатные

	средства ТЗКИ и контроля защищенности информации, осуществлять контроль защищенности информации; устанавливать, монтировать, устранять неисправности оборудования для обеспечения ТЗКИ, контролировать оснащенность объекта защиты; проводить организационные и технические мероприятия по ТЗКИ Владеть: организации деятельности подразделений и специалистов в области ТЗКИ в органах государственной власти и организациях; работы с действующей нормативной правовой и методической базой в области защиты информации; разработки необходимой документации по вопросам организации ТЗКИ в органах государственной власти и организациях; выявления ТКУИ и определения угроз безопасности информации применительно к конкретным объектам защиты

ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины **«Информационная безопасность»** составляет 256 часов.

Распределение трудоемкости дисциплины по видам занятий

Очно-заочная форма обучения с применением дистанционных образовательных технологий

Вид учебной работы	Всего часов
Аудиторные занятия (всего)	250
Лекции	221
Консультации (К)	29
Лабораторные работы (ЛР),	-
Самостоятельная работа	232
Контроль	24
Общая трудоемкость час	256

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Содержание разделов дисциплины и распределение трудоемкости по видам занятий

Очно-заочная форма обучения применением дистанционных образовательных технологий

№ п/п	Наименование темы	Содержание раздела	Лекц	К.	Лаб. зан.	СРС	Всего, час
1	Основные понятия теории информационной безопасности Информация как объект защиты Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	Основные понятия теории информационной безопасности Информация как объект защиты Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	15	5		70	92
2	Угрозы информационной безопасности	Угрозы информационной безопасности Построение систем защиты от	10	4		60	76

	Построение систем защиты от угрозы нарушения конфиденциальности Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	угрозы нарушения конфиденциальности Построение систем защиты от угрозы нарушения целостности информации и отказа доступа					
3	Политика и модели безопасности Обзор международных стандартов информационной безопасности Информационные войны и информационное противоборство	Политика и модели безопасности Обзор международных стандартов информационной безопасности Информационные войны и информационное противоборство	20			70	92
4	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ. ТРАДИЦИОННЫЙ ПОДХОД К АНАЛИЗУ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТНО-ОРИЕНТИРОВАННЫЙ ПОДХОД – ПЕРСПЕКТИВНЫЙ ПРИНЦИП АНАЛИЗА ВОПРОСОВ ИНФОРМАЦИО	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ. ТРАДИЦИОННЫЙ ПОДХОД К АНАЛИЗУ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТНО-ОРИЕНТИРОВАННЫЙ ПОДХОД – ПЕРСПЕКТИВНЫЙ ПРИНЦИП АНАЛИЗА ВОПРОСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	18	4		70	94

	ННОЙ БЕЗОПАСНОСТИ						
5	ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И КРИТЕРИИ КЛАССИФИКАЦИИ УГРОЗ УРОВНИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И КРИТЕРИИ КЛАССИФИКАЦИИ УГРОЗ УРОВНИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	25	4		75	106
6	АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕДУРНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОСНОВНЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕДУРНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОСНОВНЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	25	10		83	120
7	КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ	КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ ВРЕДОНОСТНЫЕ ПРОГРАММЫ	30			80	112

	СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ ВРЕДОНОСТНЫЕ ПРОГРАММЫ						
8	ОСНОВЫ БОРЬБЫ С ВРЕДОНОСТНЫМИ ПРОГРАММАМИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГЛОБАЛЬНЫХ СЕТЯХ МЕХАНИЗМЫ РЕАЛИЗАЦИИ УДАЛЕННЫХ АТАК В ГЛОБАЛЬНОЙ СЕТИ INTERNET	ОСНОВЫ БОРЬБЫ С ВРЕДОНОСТНЫМИ ПРОГРАММАМИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГЛОБАЛЬНЫХ СЕТЯХ МЕХАНИЗМЫ РЕАЛИЗАЦИИ УДАЛЕННЫХ АТАК В ГЛОБАЛЬНОЙ СЕТИ INTERNET	30	2		80	114
9	ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМ ВХОДЯЩИХ В СОСТАВ ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ ОБЕСПЕЧЕНИЕ БЕЗОПАСТНОГО ВЗАИМОДЕЙСТВИЯ В ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОПЕРАЦИОННЫХ СИСТЕМАХ И ПРОГРАММНОМ ОБЕСПЕЧЕНИИ	ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМ ВХОДЯЩИХ В СОСТАВ ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ ОБЕСПЕЧЕНИЕ БЕЗОПАСТНОГО ВЗАИМОДЕЙСТВИЯ В ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОПЕРАЦИОННЫХ СИСТЕМАХ И ПРОГРАММНОМ ОБЕСПЕЧЕНИИ	30			78	110

10	ОСНОВЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА UNIX БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	ОСНОВЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА UNIX БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	18			70	90
11	Итоговая аттестация	Итоговая аттестация			4		
Итого			**221**	**29**	**4**	**232**	**256**

Заочная форма обучения применением дистанционных образовательных технологий

№ п/п	Наименование темы	Содержание раздела	Общая трудоемкость	С применением дистанционных технологий			
				Консультации	Промежуточная аттестация	Итоговая аттестация	Самостоятельная работа
1	Основные понятия теории информационной безопасности Информация как объект защиты Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	Основные понятия теории информационной безопасности Информация как объект защиты Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	40	1	1		38
2	Угрозы информационной безопасности Построение систем защиты от угрозы нарушения конфиденциальн	Угрозы информационной безопасности Построение систем защиты от угрозы нарушения конфиденциальности Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	24	1	1		22

	ости Построение систем защиты от угрозы нарушения целостности информации и отказа доступа						
3	Политика и модели безопасности Обзор международных стандартов информационной безопасности Информационные войны и информационное противоборство	Политика и модели безопасности Обзор международных стандартов информационной безопасности Информационные войны и информационное противоборство	40	1	1		38
4	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ. ТРАДИЦИОННЫЙ ПОДХОД К АНАЛИЗУ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТНО-ОРИЕНТИРОВАННЫЙ ПОДХОД – ПЕРСПЕКТИВНЫЙ ПРИНЦИП АНАЛИЗА ВОПРОСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ. ТРАДИЦИОННЫЙ ПОДХОД К АНАЛИЗУ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТНО-ОРИЕНТИРОВАННЫЙ ПОДХОД – ПЕРСПЕКТИВНЫЙ ПРИНЦИП АНАЛИЗА ВОПРОСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	42	1	1		40
5	ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ	ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И КРИТЕРИИ	54	1	1		52

	И КРИТЕРИИ КЛАССИФИКАЦИИ УГРОЗ УРОВНИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	КЛАССИФИКАЦИИ УГРОЗ УРОВНИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ					
6	АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕДУРНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОСНОВНЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕДУРНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОСНОВНЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	68	1	1		66
7	КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ ВРЕДОНОСТН	КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ ВРЕДОНОСТНЫЕ ПРОГРАММЫ	60	1			58

	ЫЕ ПРОГРАММЫ						
8	ОСНОВЫ БОРЬБЫ С ВРЕДОНОСТНЫМИ ПРОГРАММАМИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГЛОБАЛЬНЫХ СЕТЯХ МЕХАНИЗМЫ РЕАЛИЗАЦИИ УДАЛЕННЫХ АТАК В ГЛОБАЛЬНОЙ СЕТИ INTERNET	ОСНОВЫ БОРЬБЫ С ВРЕДОНОСТНЫМИ ПРОГРАММАМИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГЛОБАЛЬНЫХ СЕТЯХ МЕХАНИЗМЫ РЕАЛИЗАЦИИ УДАЛЕННЫХ АТАК В ГЛОБАЛЬНОЙ СЕТИ INTERNET	62	1	1		60
9	ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМ ВХОДЯЩИХ В СОСТАВ ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ ОБЕСПЕЧЕНИЕ БЕЗОПАСТНОГО ВЗАИМОДЕЙСТВИЯ В ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОПЕРАЦИОННЫХ СИСТЕМАХ И ПРОГРАММНОМ ОБЕСПЕЧЕНИИ	ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМ ВХОДЯЩИХ В СОСТАВ ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ ОБЕСПЕЧЕНИЕ БЕЗОПАСТНОГО ВЗАИМОДЕЙСТВИЯ В ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОПЕРАЦИОННЫХ СИСТЕМАХ И ПРОГРАММНОМ ОБЕСПЕЧЕНИИ	60	1	1		58
10	ОСНОВЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ	ОСНОВЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА UNIX БЕЗОПАСНОСТЬ ПРОГРАММНОГО	38	1	1		36

	СЕМЕЙСТВА UNIX БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	ОБЕСПЕЧЕНИЯ					
11	Итоговая аттестация	Итоговая аттестация				4	
Итого			**256**	**10**	**10**	**4**	**232**

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем

HTTPS://PROFEDU.CCHGEU.RU/

Перечень учебной литературы, необходимой для освоения дисциплины

1. Аверченков, В. И. Аудит информационной безопасности органов исполнительной власти. Учебное пособие / В.И. Аверченков. - М.: Флинта, 2020. - 297 с.
2. Аверченков, В. И. Аудит информационной безопасности. Учебное пособие / В.И. Аверченков. - М.: Флинта, 2021. - 679 с.
3. Александр, Шилов und Владимир Мищенко Информационная безопасность финансового учреждения / Александр Шилов und Владимир Мищенко. - М.: LAP Lambert Academic Publishing, 2021. - 164 с.
4. Артемов, А. Информационная безопасность. Курс лекций / А. Артемов. - Москва: РГГУ, 2018. - 788 с.
5. Астахова, Людмила Герменевтика в информационной безопасности / Людмила Астахова. - М.: LAP Lambert Academic Publishing, 2020. - 296 с.
6. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: моногр. . - Москва: Мир, 2020. - 552 с.
7. Афанасьев, Алексей Алексеевич Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. Гриф УМО МО РФ / Афанасьев Алексей Алексеевич. - М.: Горячая линия - Телеком, 2020. - 438 с.
8. Бабаш, А. В. Информационная безопасность (+ CD-ROM) / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2021. - 136 с.
9. Бабаш, А. В. Информационная безопасность. Лабораторный практикум. Учебное пособие (+ CD) / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 132 с.
10. Бабаш, А.В. Информационная безопасность. История защиты информации в России / А.В. Бабаш. - М.: Книжный дом "Университет" (КДУ), 2018. - 172 с.
11. Бабаш, Александр Владимирович Информационная безопасность. Практикум. Учебное пособие для бакалавриата / Бабаш Александр Владимирович. - М.: КноРус, 2018. - 638 с.
12. Баранова, Е. К. Информационная безопасность и защита. Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: РИОР, Инфра-М, 2020. - 324 с.

ОПИСАНИЕ ПОКАЗАТЕЛЕЙ, КРИТЕРИЕВ И ШКАЛ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА ЭТАПЕ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Показатели оценивания компетенций	**Шкала и критерии оценки уровня сформированности компетенции**			
	Неудовлетворительный	**Минимально допустимый (пороговый)**	**Средний**	**Высокий**
Полнота знаний	Уровень знаний ниже минимальных требований. Имели место грубые ошибки	Минимально допустимый уровень знаний. Допущены не грубые ошибки.	Уровень знаний в объёме, соответствующем программе подготовки. Допущены некоторые погрешности.	Уровень знаний в объёме, соответствующем программе подготовки
Наличие умений	При выполнении стандартных заданий не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Выполнены типовые задания с не грубыми ошибками. Выполнены все задания, но не в полном объеме (отсутствуют пояснения, неполные выводы)	Продемонстрированы все основные умения. Выполнены все основные задания с некоторыми погрешностями. Выполнены все задания в полном объёме, но некоторые с недочетами.	Продемонстрированы все основные умения. Выполнены все основные и дополнительные задания без ошибок и погрешностей. Задания выполнены в полном объеме без недочетов.
Наличие навыков (владение опытом)	При выполнении стандартных заданий не продемонстрированы базовые навыки. Имели место грубые ошибки	Имеется минимальный набор навыков для выполнения стандартных заданий с некоторыми недочетами.	Продемонстрированы базовые навыки при выполнении стандартных заданий с некоторыми недочетами.	Продемонстрированы все основные умения. Выполнены все основные и дополнительные задания без ошибок и погрешностей. Продемонстрирован творческий подход к решению нестандартных задач.
Характеристика сформированности компетенции	Компетенция в полной мере не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач. Требуется повторное	Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач,	Сформированность компетенций в целом соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения стандартных	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных

	обучение.	но требуется дополнительная практика по большинству профессиональных задач.	профессиональных задач.	профессиональных задач.

ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ МАТЕРИАЛОВ

Вопросы (тестовые задания) для оценки результатов обучения, характеризующих сформированность компетенций

К правовым методам, обеспечивающим информационнуюбезопасность, относятся:
A) Разработка аппаратных средств обеспечения правовых данных
B) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
C) Разработка и конкретизация правовых нормативных актов обеспечения безопасности
ANSWER: C
Принципом информационной безопасности является принцип недопущения:
A) Неоправданных ограничений при работе в сети (системе)
B) Рисков безопасности сети, системы
C) Презумпции секретности
ANSWER: A
Принципом политики информационной безопасности является принцип:
A) Невозможности миновать защитные средства сети (системы)
B) Усиления основного звена сети, системы
C) Полного блокирования доступа при риск-ситуациях
ANSWER: A
Принципом политики информационной безопасности является принцип:
A) Усиления защищенности самого незащищенного звена сети (системы)
B) Перехода в безопасное состояние работы сети, системы
C) Полного доступа пользователей ко всем ресурсам сети, системы
ANSWER: A
Принципом политики информационной безопасности является принцип:
A) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
B) Одноуровневой защиты сети, системы
C) Совместимых, однотипных программно-технических средств сети, системы
ANSWER: A
К основным типам средств воздействия на компьютерную сеть относится:
A) Компьютерный сбой
B) Логические закладки («мины»)
C) Аварийное отключение питания
ANSWER: B
Когда получен спам по e-mail с приложенным файлом, следует:
A) Прочитать приложение, если оно не содержит ничего ценного – удалить
B) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
C) Удалить письмо с приложением, не раскрывая (не читая) его
ANSWER: C
Принцип Кирхгофа:
A) Секретность ключа определена секретностью открытого сообщения
B) Секретность информации определена скоростью передачи данных
C) Секретность закрытого сообщения определяется секретностью ключа
ANSWER: C
ЭЦП – это:
A) Электронно-цифровой преобразователь
B) Электронно-цифровая подпись
C) Электронно-цифровой процессор
ANSWER: B
Наиболее распространены угрозы информационной безопасности корпоративной системы:

A) Покупка нелицензионного ПО
B) Ошибки эксплуатации и неумышленного изменения режима работы системы
C) Сознательного внедрения сетевых вирусов
ANSWER: B
Наиболее распространены угрозы информационной безопасности сети:
A) Распределенный доступ клиент, отказ оборудования
B) Моральный износ сети, инсайдерство
C) Сбой (отказ) оборудования, нелегальное копирование данных
ANSWER: C
Основными источниками угроз информационной безопасности являются все указанное в списке:
A) Хищение жестких дисков, подключение к сети, инсайдерство
B) Перехват данных, хищение данных, изменение архитектуры системы
C) Хищение данных, подкуп системных администраторов, нарушение регламента работы
ANSWER: B
Наиболее распространены средства воздействия на сеть офиса:
A) Слабый трафик, информационный обман, вирусы в интернет
B) Вирусы в сети, логические мины (закладки), информационный перехват
C) Компьютерные сбои, изменение администрирования, топологии
ANSWER: B
Утечкой информации в системе называется ситуация, характеризуемая:
A) Потерей данных в системе
B) Изменением формы информации
C) Изменением содержания информации
ANSWER: A
Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
A) Целостность
B) Доступность
C) Актуальность
ANSWER: A
Угроза информационной системе (компьютерной сети) – это:
A) Вероятное событие
B) Детерминированное (всегда определенное) событие
C) Событие, происходящее периодически
ANSWER: A
Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
A) Регламентированной
B) Правовой
C) Защищаемой
ANSWER: C
Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:
A) Программные, технические, организационные, технологические
B) Серверные, клиентские, спутниковые, наземные
C) Личные, корпоративные, социальные, национальные
ANSWER: A
Окончательно, ответственность за защищенность данных в компьютерной сети несет:
A) Владелец сети
B) Администратор сети
C) Пользователь сети
ANSWER: A
Политика безопасности в системе (сети) – это комплекс:
A) Руководств, требований обеспечения необходимого уровня безопасности

B) Инструкций, алгоритмов поведения пользователя в сети
C) Нормы информационного права, соблюдаемые в сети
ANSWER: A
Наиболее важным при реализации защитных мер политики безопасности является:
A) Аудит, анализ затрат на проведение защитных мер
B) Аудит, анализ безопасности
C) Аудит, анализ уязвимостей, риск-ситуаций
ANSWER: C
Виды информационной безопасности:
A) Персональная, корпоративная, государственная
B) Клиентская, серверная, сетевая
C) Локальная, глобальная, смешанная
ANSWER: A
Цели информационной безопасности – своевременное обнаружение, предупреждение:
A) несанкционированного доступа, воздействия в сети
B) инсайдерства в организации
C) чрезвычайных ситуаций
ANSWER: A
Основная масса угроз информационной безопасности приходится на:
A) Троянские программы
B) Шпионские программы
C) Черви
ANSWER: A
Какой вид идентификации и аутентификации получил наибольшее распространение:
A) системы PKI
B) постоянные пароли
C) одноразовые пароли
ANSWER: B
Под какие системы распространение вирусов происходит наиболее динамично:
A) Windows
B) Mac OS
C) Android
ANSWER: C
Заключительным этапом построения системы защиты является:
A) сопровождение
B) планирование
C) анализ уязвимых мест
ANSWER: A
Какие угрозы безопасности информации являются преднамеренными:
A) ошибки персонала
B) открытие электронного письма, содержащего вирус
C) не авторизованный доступ
ANSWER: C
Какой подход к обеспечению безопасности имеет место:
A) теоретический
B) комплексный
C) логический
ANSWER: B
Основные объекты информационной безопасности:
A) Компьютерные сети, базы данных
B) Информационные системы, психологическое состояние пользователей
C) Бизнес-ориентированные, коммерческие системы

ANSWER: A
Системой криптографической защиты информации является:
A) BFox Pro
B) CAudit Pro
C) Крипто Про
ANSWER: C
Stuxnet — это:
A) троянская программа
B) макровирус
C) промышленный вирус
ANSWER: C
Таргетированная атака — это:
A) атака на сетевое оборудование
B) атака на компьютерную систему крупного предприятия
C) атака на конкретный компьютер пользователя
ANSWER: B
Основными рисками информационной безопасности являются:
A) Искажение, уменьшение объема, перекодировка информации
B) Техническое вмешательство, выведение из строя оборудования сети
C) Потеря, искажение, утечка информации
ANSWER: C
К основным принципам обеспечения информационной безопасности относится:
A) Экономической эффективности системы безопасности
B) Многоплатформенной реализации системы
C) Усиления защищенности всех звеньев системы
ANSWER: A
Основными субъектами информационной безопасности являются:
A) руководители, менеджеры, администраторы компаний
B) органы права, государства, бизнеса
C) сетевые базы данных, фаерволлы
ANSWER: B
К основным функциям системы безопасности можно отнести все перечисленное:
A) Установление регламента, аудит системы, выявление рисков
B) Установка новых офисных приложений, смена хостинг-компании
C) Внедрение аутентификации, проверки контактных данных пользователей
ANSWER: A

ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ МАТЕРИАЛОВ

Перечень вопросов тестовых заданий, а также иных оценочных материалов приведенных в рабочих программах дисциплин используется при итоговой аттестации. Количество вопросов из каждой дисциплине или модуля определяет руководитель программы.

Итоговая аттестация проводится в виде междисциплинарного экзамена в форме тестирования.. Возможно применение дистанционных образовательных технологий.