

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



(Подпись)

А. И. Колосов
(И.О. Фамилия)

2024 г.

(дата)

ПРОГРАММА ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ
Информационная безопасность
(наименование программы)

(наименование присваиваемой квалификации (при наличии))

СОГЛАСОВАНО:

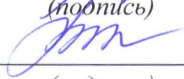
Директор ЦДПО


(подпись)

А.В. Воротынцева

(И.О. Фамилия)

Автор программы


(подпись)

Е.А. Тарасов

(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 09.09.2022 № 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 | <p>Знать: типовые структуры управления, связи и автоматизации объектов информатизации, требования к их оснащённости 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);</p> <p>Уметь: работать с действующей нормативной правовой и методической базой в области защиты информации; определять возможные ТКУИ и угрозы</p> |

| | | |
|--|--|---|
| | | <p>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;</p> <p>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</p> |
| <p>производственно-технологический</p> | <p>ПК-2 Способность использовать достижения науки и техники в области защиты информации, пользоваться реферативными и справочно-информационными изданиями в области защиты информации</p> | <p>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</p> <p>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</p> |

| | | |
|--|---|---|
| | | <p>требований по ТЗКИ</p> <p>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</p> |
| <p>производственно-технологический</p> | <p>ПК-3 Способность определять возможные ТКУИ и угрозы безопасности информации на основе анализа информационных процессов в организации, целей и задач деятельности объекта защиты</p> | <p>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</p> <p>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</p> <p>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</p> |

| | | |
|--|--|--|
| | | 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 профессиональное образование или является студентом последнего курса обучения.

1.5. Трудоемкость обучения - _____ 1010 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

(И.О. Фамилия)

2024 г.

(подпись)

« »

УЧЕБНЫЙ ПЛАН

Информационная безопасность

(наименование присваиваемой квалификации (при наличии))

СОГЛАСОВАНО:

Директор ЦДПО

Автор программы

(подпись)

А.В. Воротынцева

(И.О. Фамилия)

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: 1010 часов

Режим занятий: 8 часов в день, 6 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 | 92 | 15 | 5 | 2 | | 70 | - |
| Угрозы информационной безопасности Построение систем защиты от угрозы нарушения конфиденциальности Построение систем защиты от угрозы нарушения целостности информации и отказа доступа | 76 | 10 | 4 | 2 | | 60 | - |
| Политика и модели безопасности Обзор международных стандартов информационной безопасности Информационные войны и информационное противоборство | 92 | 20 | | 2 | | 70 | - |
| ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ | 94 | 18 | 4 | 2 | | 70 | - |

| 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 | 106 | 25 | 4 | 2 | | 75 | - |
| АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕДУРНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОСНОВНЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ | 120 | 25 | 10 | 2 | | 83 | - |
| КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ ВРЕДНОСТНЫЕ ПРОГРАММЫ | 112 | 30 | | 2 | | 80 | - |
| ОСНОВЫ БОРЬБЫ С ВРЕДНОСТНЫМИ ПРОГРАММАМИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГЛОБАЛЬНЫХ СЕТЯХ | 114 | 30 | 2 | 2 | | 80 | - |

| 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 БЕЗОПАСНОГО ВЗАИМОДЕЙСТВИЯ В ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОПЕРАЦИОННЫХ СИСТЕМАХ И ПРОГРАММНОМ ОБЕСПЕЧЕНИИ | 110 | 30 | | 2 | | 78 | - |
| ОСНОВЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА UNIX БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ | 90 | 18 | | 2 | | 70 | - |
| Итоговая аттестация | 4 | | | | 4 | | - |
| ИТОГО: | 1010 | 221 | 29 | 20 | 4 | 736 | |

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: 1010 часов

Режим занятий: 8 часов в день, 6 месяцев

Форма обучения: заочная с применением дистанционных образовательных технологий.

Форма организации учебного процесса: модульная

Уровень образования: высшее, средне профессиональное

Общая трудоемкость: 28 зачетные единицы, 1010 часов, в том числе с применением дистанционных технологий 1010 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 | 92 | 1 | 1 | | 90 |
| Угрозы информационной безопасности Построение систем защиты от угрозы нарушения конфиденциальности Построение систем защиты от угрозы нарушения целостности информации и отказа доступа | 76 | 1 | 1 | | 74 |
| Политика и модели безопасности Обзор международных стандартов информационной безопасности Информационные войны и информационное противоборство | 92 | 1 | 1 | | 90 |
| ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ. | 94 | 1 | 1 | | 92 |

| 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 | 106 | 1 | 1 | | 104 |
| АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕДУРНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОСНОВНЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ | 120 | 1 | 1 | | 118 |
| КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ ВРЕДНОСТНЫЕ ПРОГРАММЫ | 112 | 1 | 1 | | 110 |
| ОСНОВЫ БОРЬБЫ С ВРЕДНОСТНЫМИ | 114 | 1 | 1 | | 112 |

| 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 БЕЗОПАСНОГО ВЗАИМОДЕЙСТВИЯ В ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОПЕРАЦИОННЫХ СИСТЕМАХ И ПРОГРАММНОМ ОБЕСПЕЧЕНИИ | 110 | 1 | 1 | | 108 |
| ОСНОВЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА UNIX БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ | 90 | 1 | 1 | | 88 |
| Итоговая аттестация | 4 | | | 4 | |
| ИТОГО: | 1010 | 10 | 10 | 4 | 986 |

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 использованием 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
(И.О. Фамилия)

2024 г.

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

*Дополнительная профессиональная программа
(профессиональная переподготовка)*

Информационная безопасность

(наименование присваиваемой квалификации (при наличии))

СОГЛАСОВАНО:

Директор ЦДПО

Автор программы



(подпись)

А.В. Воротынцева

(И.О. Фамилия)

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 профессиональное образование или являются студентами последнего курса обучения.

Срок обучения: 1010 часов

Режим занятий: 8 часов в день, 6 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 | 92 | 15 | 5 | 2 | | 70 | - |
| Угрозы информационной безопасности Построение систем защиты от угрозы нарушения конфиденциальности Построение систем защиты от угрозы нарушения целостности информации и отказа доступа | 76 | 10 | 4 | 2 | | 60 | - |
| Политика и модели безопасности Обзор международных стандартов информационной безопасности Информационные войны и информационное противоборство | 92 | 20 | | 2 | | 70 | - |
| ОСНОВЫ ИНФОРМАЦИОННОЙ | 94 | 18 | 4 | 2 | | 70 | - |

| 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 | 106 | 25 | 4 | 2 | | 75 | - |
| АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕДУРНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОСНОВНЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ | 120 | 25 | 10 | 2 | | 83 | - |
| КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ ВРЕДНОСТНЫЕ ПРОГРАММЫ | 112 | 30 | | 2 | | 80 | - |
| ОСНОВЫ БОРЬБЫ С ВРЕДНОСТНЫМИ ПРОГРАММАМИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В | 114 | 30 | 2 | 2 | | 80 | - |

| 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 БЕЗОПАСНОГО ВЗАИМОДЕЙСТВИЯ В ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОПЕРАЦИОННЫХ СИСТЕМАХ И ПРОГРАММНОМ ОБЕСПЕЧЕНИИ | 110 | 30 | | 2 | | 78 | - |
| ОСНОВЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА UNIX БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ | 90 | 18 | | 2 | | 70 | - |
| Итоговая аттестация | 4 | | | | 4 | | - |
| ИТОГО: | 1010 | 221 | 29 | 20 | 4 | 736 | |

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: 1010 часов

Режим занятий: 8 часов в день, 6 месяцев

Форма обучения: заочная с применением дистанционных образовательных технологий.

Форма организации учебного процесса: модульная

Уровень образования: высшее, средне профессиональное

Общая трудоемкость: 28 зачетные единицы, 1010 часов, в том числе с применением дистанционных технологий 1010 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 | 92 | 1 | 1 | | 90 |
| Угрозы информационной безопасности Построение систем защиты от угрозы нарушения конфиденциальности Построение систем защиты от угрозы нарушения целостности информации и отказа доступа | 76 | 1 | 1 | | 74 |
| Политика и модели безопасности Обзор международных стандартов информационной безопасности Информационные войны и информационное противоборство | 92 | 1 | 1 | | 90 |
| ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ. | 94 | 1 | 1 | | 92 |

| 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 | 106 | 1 | 1 | | 104 |
| АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕДУРНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОСНОВНЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ | 120 | 1 | 1 | | 118 |
| КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ АСИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ ВРЕДНОСТНЫЕ ПРОГРАММЫ | 112 | 1 | 1 | | 110 |
| ОСНОВЫ БОРЬБЫ С ВРЕДНОСТНЫМИ | 114 | 1 | 1 | | 112 |

| 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 БЕЗОПАСНОГО ВЗАИМОДЕЙСТВИЯ В ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОПЕРАЦИОННЫХ СИСТЕМАХ И ПРОГРАММНОМ ОБЕСПЕЧЕНИИ | 110 | 1 | 1 | | 108 |
| ОСНОВЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА UNIX БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ | 90 | 1 | 1 | | 88 |
| Итоговая аттестация | 4 | | | 4 | |
| ИТОГО: | 1010 | 10 | 10 | 4 | 986 |

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 использованием 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)

1010 часов

СОГЛАСОВАНО:

Директор ЦДПО



(подпись)

А.В. Воротынцева

(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.