МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Учебный центр ИПиПК ВолгГТУ

«Цифровая кафедра»

УЧЕБНЫЙ ПЛАН
ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

“*Кибербезопасность (CyberSecurity)*”

Цель	Программа переподготовки “ Кибербезопасность” объемом 252 часа разработана в рамках реализации проекта “Цифровая кафедра” программы Приоритет 2030. Для успешного освоения курса необходимо проходить обучение или иметь высшее образование по ИТ направлению. Освоение программы в полном объеме позволяет слушателям повысить уровень профессиональных знаний и получить практические навыки работы в области информационных технологий: обеспечение безопасности информации в автоматизированных системах; приобретение новой квалификации – «Специалист по защите информации в автоматизированных системах».
Категория слушателей	Студенты бакалавриата, специалитета, магистратуры, аспирантуры, профессорско-преподавательский состав, специалисты,другие категории.
Срок обучения	9 месяцев
Форма обучения	с отрывом, без отрыва от производства и с частичным отрывом от производства
Режим занятий	6-8 часов в день при очной, очно-заочной, дистанционной формах обучения

Волгоград 2022

Индекс	Наименование учебной дисциплины	Общая трудоемкость	Всего ауд.час.	Количество ауд.(академических) часов			Самост. работа	Контроль
				Лекции	Лабораторные работы	Практика		
	1-ый семестр	108	32	16	16	16	44	16
1.	Цели и задачи ИБ. Защищаемые информация и информационные ресурсы. Объекты защиты	1,1	1	1				0,1 зачет
2.	Определение угроз безопасности информации ограниченного доступа	5,1	3	1	2		2	0,1 зачет
3.	Основы нормативного правового обеспечения ИБ	6,2	4	2	2		2	0,2 зачет
4.	Средства и системы обработки информации	24,2	8	4	4		16	0,2 зачет
5.	Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам	24,2	8	4	4		16	0,2 зачет
7.	Угрозы безопасности информации, связанные с НСД	16,2	8	4	4		8	0,2 зачет
8.	Практика	16,2				16		0,2 зачет

9.	Промежуточная аттестация	14,8	0					14,8 зачет
	2-ой семестр	144	32	16	16	56	40	16
6.	Меры и средства защиты информации от НСД	12,2	4	2	2		8	0,2 зачет
8.	Информация как объект защиты от специальных воздействий	20,2	8	4	4		12	0,2 зачет
9.	Организация защиты конфиденциальной информации на объектах информатизации	20,2	8	4	4		12	0,2 зачет
10.	Аттестация объектов информатизации по требованиям безопасности информации	6,2	4	2	2		2	0,2 зачет
11.	Контроль состояния технической защиты конфиденциальной информации	14,2	8	4	4		6	0,2 зачет
12.	Практика	32,2				32		0,2 зачет
13.	Итоговая аттестация	38,8				24		14,8 зачет
Всего		252	64	32	32	72	84	32

Директор ИП и ПК В. В. Шеховцов

Директор УЦ «Цифровая кафедра» А.Г. Кравец

МИНИСТЕРСТВО НАУКИ и ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УЧЕБНЫЙ ЦЕНТР ИП и ПК ВолгГТУ

«ЦИФРОВАЯ КАФЕДРА»

«УТВЕРЖДАЮ»
Первый проректор ВолгГТУ
_____ С.В. Кузьмин
«11» _____ 2022 г.

ПРОГРАММА
профессиональной переподготовки
“КИБЕРБЕЗОПАСНОСТЬ”

Всего часов по учебному плану	252
Всего аудиторных занятий	64
Лекции	32
Лабораторные работы	32
Самостоятельная работа	84
Практика	72
Контроль	32

Волгоград 2022

Директор ИП и ПК В.В. Шеховцов

Директор УЦ «ЦК»,
д.т.н., профессор. каф. ВТ А.Г. Кравец

Разработчики программы:

Зам. директора ИПиПК А.А. Алпатов

Одобрена комиссией по ДО НМС ВолгГТУ
Протокол № 5 от «29» 06 2022 г.

Оглавление

ВВЕДЕНИЕ

Дополнительная профессиональная программа (программа профессиональной переподготовки) ИТ-профиля «Кибербезопасность» (далее – Программа) разработана в соответствии с нормами Федерального закона РФ от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации», с учетом требований приказа Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», с изменениями, внесенными приказом Минобрнауки России от 15 ноября 2013 г. № 1244 «О внесении изменений в Порядок организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденный приказом Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499», приказа Министерства образования и науки РФ от 23 августа 2017 г. N 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ» (указать при необходимости); паспорта федерального проекта «Развитие кадрового потенциала ИТ-отрасли» национальной программы «Цифровая экономика Российской Федерации»; постановления Правительства Российской Федерации от 13 мая 2021 г. № 729 «О мерах по реализации программы стратегического лидерства «Приоритет-2030» (в редакции постановления Правительства Российской Федерации от 14 марта 2022 г. № 357 «О внесении изменений в постановление Правительства Российской Федерации от 13 мая 2021 г. № 729»); приказа Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 28 февраля 2022 г. № 143 «Об утверждении методик расчета показателей федеральных проектов национальной программы «Цифровая экономика Российской Федерации» и признании утратившими силу некоторых приказов Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации об утверждении методик расчета показателей федеральных проектов национальной программы «Цифровая экономика Российской Федерации» (далее – приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации № 143); федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.01 Информатика и вычислительная техника (уровень бакалавриата), утвержденного приказом Минобрнауки России от 12 января 2016 г. № 5, (далее вместе – ФГОС ВО)), а также профессионального стандарта «Специалист по защите информации в автоматизированных системах» утвержденного приказом Министерства труда и социальной защиты РФ от 15 сентября 2016 г. № 522н.

Профессиональная переподготовка заинтересованных лиц (далее – Слушатели), осуществляемая в соответствии с Программой (далее – Подготовка), имеющей отраслевую направленность «Информационно-коммуникационные технологии»,

проводится в Волгоградском государственном техническом университете (далее – Университет) в соответствии с учебным планом в очной/заочной форме обучения.
Разделы, включенные в учебный план Программы, используются для последующей разработки календарного учебного графика, учебно-тематического плана, рабочей программы, оценочных и методических материалов. Перечисленные документы разрабатываются Университетом самостоятельно, с учетом актуальных положений законодательства об образовании, законодательства в области информационных технологий и смежных областей знаний ФГОС ВО и профессионального стандарта «Специалист по защите информации в автоматизированных системах» (06.033) утвержденного приказом Министерства труда и социальной защиты РФ от 15 сентября 2016 г. № 522н.
Программа регламентирует требования к профессиональной переподготовке в области управление работами по созданию (модификации) и сопровождению информационных ресурсов.
Срок освоения Программы составляет 7 зачетных единиц (252 часов).
К освоению Программы в рамках проекта допускаются лица:
- получающие высшее образование по очной (очно-заочной) форме, лица, освоившие основную профессиональную образовательную программу (далее – ОПОП ВО) бакалавриата – в объеме не менее первого курса (бакалавры 2-го курса), ОПОП ВО специалитета – не менее первого и второго курсов (специалисты 3-го курса), а также магистратуры, обучающиеся по ОПОП ВО, отнесенным к ИТ-сфере.
Область профессиональной деятельности «Информационно-коммуникационные технологии» (ИКТ).

II. ЦЕЛЬ

Целью подготовки слушателей по Программе является получение компетенции, необходимой для выполнения нового вида профессиональной деятельности в области Обеспечение безопасности информации в автоматизированных системах; приобретение новой квалификации – «Специалист по защите информации в автоматизированных системах» информационных технологий.
Целью подготовки слушателей по Программе является обеспечение безопасности информации в автоматизированных системах, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите.

III.ХАРАКТЕРИСТИКА НОВОЙ КВАЛИФИКАЦИИ И СВЯЗАННЫХ С НЕЙ ВИДОВ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ, ТРУДОВЫХ ФУНКЦИЙ И (ИЛИ) УРОВНЕЙ КВАЛИФИКАЦИИ

Виды профессиональной деятельности, трудовая функция, указанные в профессиональном стандарте по соответствующей должности «Инженер по защите информации» представлены в таблице 1. Характеристика новой и развиваемой цифровой компетенции в ИТ-сфере представлены в таблице 2.

Таблица 1

Характеристика новой квалификации, связанной с видом профессиональной деятельности и трудовыми функциями в соответствии с профессиональным стандартом «Специалист по защите информации в автоматизированных системах» (06.033)

Область профессиональной деятельности	Тип задач профессиональной деятельности	Код и наименование профессиональной компетенции	Трудовые действия	Трудовая функция	Обобщенная трудовая функция	Вид профессиональной деятельности
ИКТ	Обеспечение безопасности информации в автоматизированных системах, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите	ПК-1 применяет языки программирования для решения профессиональных задач ПК-2 Применяет принципы и основы алгоритмизации ПК-3 Применяет СУБД ПК-4 Применяет программное обеспечение для защиты информации	Установка обновлений программного обеспечения автоматизированной системы. Обеспечение безопасности информации с учетом требования эффективного функционирования автоматизированной системы. Управление полномочиями пользователей автоматизированной системы. Информирование пользователей о правилах эксплуатации автоматизированной системы с учетом требований по защите информаци. Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий с персоналом на макетах или в тестовой зоне. Внесение изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы.	Администрирование систем защиты информации автоматизированных систем	Обеспеч ние защиты информации в автоматизированных системах в процессе их эксплуатации	Обеспечение безопасности информации в автоматизированных системах

Таблица 2

Характеристика новой и развиваемой цифровой компетенции в ИТ-сфере, связанной с уровнем формирования и развития в результате освоения Программы «Кибербезопасность».

Наименование сферы	Код и наименование профессиональной компетенции	Пример инструментов	0 — способность не проявляется/ проявляется в степени, недостаточной для отнесения к 1 уровню сформированности компетенции	1 — способность проявляется под внешним контролем / при внешней постановке задачи/ обучающийся пользуется готовыми, рекомендованными продуктами	2 — способность проявляется, но обучающийся эпизодически прибегает к экспертной консультации/ самостоятельно подбирает и пользуется готовыми продуктами	3 — способность проявляется системно / обучающийся модифицирует способность под определенные задачи / создает новый продукт, обучает других
ИКТ	ПК-4 Применяет программное обеспечение для защиты информации	Инструменты-Антивирусы, firewall, Dr.Web, Kaspersky и т.д	(-)	(+)	(+)	(+)

IV. ХАРАКТЕРИСТИКА НОВЫХ И РАЗВИВАЕМЫХ ЦИФРОВЫХ КОМПЕТЕНЦИЙ, ФОРМИРУЮЩИХСЯ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ПРОГРАММЫ

В ходе освоения Программы Слушателем приобретаются/совершенствуются следующие профессиональные компетенции:
ПК-4 Применяет программное обеспечение для защиты информации

V. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДПП ПП

Результатами подготовки слушателей по Программе является получение компетенции, необходимой для выполнения нового вида профессиональной деятельности в области информационных технологий: обеспечение безопасности информации в автоматизированных системах; приобретение новой квалификации – «Специалист по защите информации в автоматизированных системах».
В результате освоения Программы слушатель должен:
Знать:

- нормативные правовые акты, методические документы, международные и национальные стандарты в области ИБ;
- основы функционирования государственной системы противодействия (ПД) иностранным техническим разведкам (ИТР) и ТЗИ, цели и задачи ИБ;
- виды конфиденциальной информации, перечни сведений конфиденциального характера;
- возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий;
- действующую систему сертификации средств защиты информации по требованиям безопасности информации;
- основы лицензирования деятельности по ИБ;
- требования по ИБ (нормы, требования и рекомендации по защите объектов информатизации, методы и методики контроля (мониторинга) их выполнения);
- организацию и содержание проведения работ по ИБ, состав и содержание необходимых документов;
- организацию и содержание проведения работ по контролю(мониторингу) защищенности конфиденциальной информации, состав и содержание необходимых документов;
- правила разработки, утверждения, обновления и отмены документов в области ИБ;
- типовую структуру, задачи и полномочия подразделения по ТЗИ;
- принципы работы основных узлов современных технических средств информатизации;
- основы построения информационных систем и формирования информационных ресурсов, принципы построения и функционирования операционных систем, систем управления базами данных, локальных и глобальных компьютерных сетей, основные протоколы компьютерных сетей;

- типовые структуры управления, связи и автоматизации объектов информатизации, требования к их оснащенности техническими средствами;
- технические каналы утечки информации, возникающие при ее обработке техническими средствами и системами;
- способы (методы) и требования по ИБ;
- подсистемы разграничения доступа, подсистемы обнаружения атак, подсистемы защиты информации от утечки по техническим каналам, несанкционированных, непреднамеренных воздействий, контроля целостности информации;
- порядок осуществления аутентификации взаимодействующих объектов, проверки подлинности отправителя и целостности передаваемых данных;
- методы и методики контроля (мониторинга) защищенности конфиденциальной информации;
- порядок проведения контроля (мониторинга) информационной безопасности средств и систем информатизации;
- требования к средствам ИБ и средствам контроля (мониторинга) эффективности мер защиты информации;
- средства ИБ и средствам контроля (мониторинга) эффективности мер защиты информации, порядок их применения, перспективы развития;
- порядок проведения аттестационных испытаний и аттестации объектов информатизации на соответствие требованиям по защите информации;
- порядок, содержание, условия и методы испытаний для оценки характеристик и показателей, проверяемых при аттестации, соответствия их установленным требованиям, а также применяемую в этих целях контрольную аппаратуру и тестовые средства;
- программы и методики аттестационных испытаний и аттестации объекта информатизации на соответствие требованиям по защите информации;
- порядок установки, монтажа, испытаний средств ИБ+ и средств контроля (мониторинга) эффективности мер защиты информации;
- порядок устранения неисправностей и проведения ремонта (технического обслуживания) средств ИБ и средств контроля (мониторинга) эффективности мер защиты информации;

Уметь:

- применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области ИБ;
- разрабатывать необходимые документы в интересах проведения работ по ИБ;
- определять возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий;
- формировать требования по ИБ;
- определять требования к средствам ИБ на объектах информатизации;
- организовывать и проводить работы по ИБ;
- организовывать и проводить работы по контролю (мониторингу) защищенности конфиденциальной информации, оформлять материалы по результатам контроля;
- применять на практике штатные средства ИБ и средства контроля (мониторинга) эффективности мер защиты информации;

- проводить аттестационные испытания и аттестацию объектов информатизации на соответствие требованиям по защите информации, оформлять материалы аттестационных испытаний;
- разрабатывать программы и методики аттестационных испытаний и аттестации объектов информатизации;
- осуществлять аутентификацию взаимодействующих объектов, проверку подлинности отправителя и целостности передаваемых данных;
- проводить установку, монтаж, испытания и техническое обслуживание средств ИБ и средств контроля (мониторинга) эффективности мер защиты информации;
- устранять неисправности и проводить ремонт (техническое обслуживание) средств ИБ и средств контроля (мониторинга) эффективности мер защиты информации;
- разрабатывать документы для получения лицензии на проведение работ и оказания услуг по ИБ для их представления в лицензирующий орган;

Иметь навыки:

- работы с действующей нормативной правовой и методической базой в области ТЗИ;
- выявления ТКУИ и определения угроз безопасности информации;
- определения задач, проведения организационных и технических мероприятий по ИБ;
- определения задач, проведения организационных и технических мероприятий по контролю (мониторингу) защищенности конфиденциальной информации, подготовки материалов по результатам контроля;
- применения средств ИБ и средств контроля (мониторинга) эффективности мер защиты информации;
- работы в компьютерных сетях с учетом требований по безопасности информации;
- работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения, в том числе зарубежными информационными ресурсами;
- проведения аттестационных испытаний и аттестаций объектов информатизации на соответствие требованиям по защите информации, оформления материалов аттестационных испытаний;
- организации деятельности подразделений и специалистов в области ИБ;
- проведения установки, монтажа, испытания средств ИБ и средств контроля (мониторинга) эффективности мер защиты информации;
- устранения неисправности и проведения ремонта (технического обслуживания) средств ИБ и средств контроля (мониторинга) эффективности мер защиты информации.

VI. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ДПП

Реализация Программы должна обеспечить получение компетенции, необходимой для выполнения нового вида профессиональной деятельности в области

информационных технологий: обеспечение безопасности информации в автоматизированных системах; приобретение новой квалификации – «Специалист по защите информации в автоматизированных системах».

Учебный процесс организуется с применением электронного обучения, дистанционных образовательных технологий; инновационных технологий и методик обучения, способных обеспечить получение слушателями знаний, умений и навыков в области информационной безопасности.

Реализация Программы обеспечивается научно-педагогическими кадрами Университета, допустимо привлечение к образовательному процессу высококвалифицированных специалистов ИТ-сферы и/или дополнительного профессионального образования в части, касающейся профессиональных компетенций в области создания алгоритмов и программ, пригодных для практического применения, с обязательным участием представителей профильных организаций-работодателей. Возможно привлечение региональных руководителей цифровой трансформации (отраслевых ведомственных и/или корпоративных) к проведению итоговой аттестации, привлечение работников организаций реального сектора экономики субъектов Российской Федерации.

VII. УЧЕБНЫЙ ПЛАН ДПП

Объем Программы составляет 252 аудиторных часов (7 зет).

Учебный план Программы определяет перечень, последовательность, общую трудоемкость разделов и формы контроля знаний.

Учебный план программы профессиональной переподготовки «Кибербезопасность» представлен в таблице 3.

Таблица 3

№ п/п	Наименование раздела (модуля)	Общая трудоемкость (252 ч)	Форма контроля
	1-ый семестр	108	Зачет
1	Цели и задачи ИБ. Защищаемые информация и информационные ресурсы. Объекты защиты	1,1	Зачет
2	Определение угроз безопасности информации ограниченного доступа	5,1	Зачет
3	Основы нормативного правового обеспечения ИБ	6,2	Зачет
4	Средства и системы обработки информации	24,2	Зачет
5	Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам	24,2	Зачет
6	Угрозы безопасности информации, связанные с НСД	16,2	Зачет

7	Практика	16,2	Зачет
8	Промежуточная аттестация	14,8	Зачет
	2-ой семестр	144	
9	Меры и средства защиты информации от НСД	12,2	Зачет
10	Информация как объект защиты от специальных воздействий	20,2	Зачет
11	Организация защиты конфиденциальной информации на объектах информатизации	20,2	Зачет
12	Аттестация объектов информатизации по требованиям безопасности информации	6,2	Зачет
13	Контроль состояния технической защиты конфиденциальной информации	14,2	Зачет
14	Практика	32,2	Зачет
15	Итоговая аттестация	38,8	Зачет
	Итого	252	

VIII. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Календарный учебный график представляет собой график учебного процесса, устанавливающий последовательность и продолжительность обучения и итоговой аттестации по учебным дням.

Календарный учебный график программы профессиональной переподготовки «Кибербезопасность» представлен в таблице 4.

Таблица 4

Дидактические единицы	Объем в часах	Сроки реализации (со дня начала занятий)
1-ый семестр		
Цели и задачи ИБ. Защищаемые информация и информационные ресурсы. Объекты защиты	1,1	1-я неделя
Определение угроз безопасности информации ограниченного доступа	5,1	2-я неделя
Основы нормативного правового обеспечения ИБ	6,2	3-я недели
Средства и системы обработки информации	24,2	4-6-я недели
Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам	24,2	7-9-я недели
Угрозы безопасности информации, связанные с НСД	16,2	10-11-я недели
Практика	16,2	12-13-я недели
Промежуточная аттестация	14,8	14-15-я недели

2-ой семестр		
Меры и средства защиты информации от НСД	12,2	16-17-я недели
Информация как объект защиты от специальных воздействий	20,2	18-20-я недели
Организация защиты конфиденциальной информации на объектах информатизации	20,2	21-23-я недели
Аттестация объектов информатизации по требованиям безопасности информации	6,2	24-я неделя
Контроль состояния технической защиты конфиденциальной информации	14,2	25-26-я недели
Практика	32,2	27-31-я недели
Итоговая аттестация	38,8	31-36-я недели
Всего	252	8 месяцев

IX. РАБОЧАЯ ПРОГРАММА УЧЕБНЫХ ПРЕДМЕТОВ ПРОГРАММЫ

Рабочая программа содержит перечень разделов и тем, а также рассматриваемых в них вопросов с учетом их трудоемкости (табл.5).

Рабочая программа разрабатывается Университетом с учетом профессионального стандарта «Специалист по защите информации в автоматизированных системах» (06.033)

Таблица 5

Наименование учебных модулей (Основные темы: Краткое содержание)	Объем, часов
1-ый семестр	
Цели и задачи ИБ. Защищаемые информация и информационные ресурсы. Объекты защиты Основные термины и определения в области ИБ. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации. Цели и задачи ИБ. Объекты информатизации: классификация и характеристика. Защищаемые информация и информационные ресурсы. Объекты защиты конфиденциальной информации. Государственные информационные ресурсы, негосударственные информационные ресурсы, находящиеся в ведении органов государственной власти и организаций. Перечень сведений конфиденциального характера, подлежащих защите.	1,1
Определение угроз безопасности информации ограниченного доступа Угрозы безопасности конфиденциальной информации. Классификация ТКУИ. Классификация угроз безопасности информации, связанных с НСД. Модель угроз безопасности информации в заданных условиях функционирования объекта защиты. Методы выявления и оценки возможности реализации угроз безопасности информации.	5,1
Основы нормативного правового обеспечения ИБ Нормативные правовые акты Российской Федерации. Нормативные правовые акты ФСТЭК России. Методические документы. Технические документы (документация). Плановые документы. Информационные документы. Документы в области технического регулирования и стандартизации. Система стандартов в области защиты информации. Стандарты Единой системы конструкторской документации (ЕСКД), Единой системы технологической документации (ЕСТД) и Единой системы	6,2

программной документации (ЕСПД). Основы лицензирования деятельности по ТЗКИ, аттестации объектов информатизации по требованиям безопасности информации. Система сертификации средств защиты информации. Ответственность за правонарушения в области защиты информации. Требования по защите конфиденциальной информации на объекте информатизации (от утечки по техническим каналам, от НСД и специальных воздействий). Особенности защиты персональных данных. Требования международных и национальных стандартов по защите информации.	
Средства и системы обработки информации Информация: основные термины и определения. Сбор и обработка информации. Информационные процессы. Технические средства обработки информации. Классификация технические средства обработки информации. Устройства хранения информации. Устройства памяти. Виды памяти. Основные типы и принцип работы клавиатуры, манипулятора «мышь», джойстика и др. устройств. Основные типы, принципы работы и технические характеристики мониторов. Типы, основные компоненты и характеристики видеоадаптеров. Принцип (способы) формирования изображения. Классификация сканеров. Обзор основных современных моделей сканеров и их технических характеристик. Назначение и краткая характеристика сетевого оборудования: кабельная система, сетевые адаптеры, концентраторы, коммутаторы, принт-серверы. Типы модемов, принцип и режимы работы. Основные принципы установки, монтажа, наладки и ремонта технических средств обработки информации	24,2
Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам Нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗКИ, цели и задачи ТЗКИ. Термины и определения в области ТЗКИ от утечки по техническим каналам: объект информатизации, защищаемое помещение, основные технические средства и системы (ОТСС), вспомогательные технические средства и системы (ВТСС), случайные антенны, контролируемая зона, ТКУИ. Физические основы возникновения ТКУИ и общая характеристика ТКУИ, обрабатываемой техническими средствами. Технический канал утечки информации за счет побочных электромагнитных излучений (ПЭМИ) средств вычислительной техники (СВТ). Схема ТКУИ, возникающего за счет ПЭМИ СВТ. Характеристики ПЭМИ СВТ в различных режимах работы. Зона 2. Принципы построения средств перехвата ПЭМИ СВТ.Технический канал утечки информации за счет наводок, возникающих под воздействием ПЭМИ СВТ. Случайные антенны. Характеристики случайных антенн. Схема ТКУИ, возникающего за счет наводок ПЭМИ СВТ в случайных антеннах Зона 1. Просачивание сигналов в линии электропитания и заземления СВТ. Схемы ТКУИ, возникающих за счет просачивания информативных сигналов в линии электропитания и заземления СВТ. Технический канал утечки информации, использующий электронные устройства съема информации («закладочные устройства»), внедряемые в СВТ. Физические основы возникновения технических каналов утечки акустической речевой информации. Акустические сигналы. Спектр и типовые уровни речевого сигнала. Классификация технических каналов утечки акустической речевой информации. Прямой акустический канал утечки акустической речевой информации из защищаемых помещений. Схемы перехвата информации по прямому акустическому каналу. Средства перехвата акустической речевой информации, использующие микрофоны воздушной проводимости. Вибрационный канал утечки акустической речевой информации из защищаемых помещений. Схемы перехвата акустической речевой информации по вибрационному каналу. Средства перехвата акустической речевой информации, использующие	24,2

вибропреобразователи. Оптико-электронный канал утечки акустической речевой информации из защищаемых помещений. Схема перехвата акустической речевой информации по оптико-электронному каналу. Средства перехвата акустической речевой информации, использующие «лазерные микрофоны». Акустоэлектрический канал утечки акустической речевой информации из защищаемых помещений. Схема пассивного акустоэлектрического канала утечки акустической речевой информации. Схема активного акустоэлектрического канала утечки акустической речевой информации. Средства перехвата акустической речевой информации, использующие эффект акустоэлектрического преобразования речевого сигнала. Акустоэлектромагнитный канал утечки акустической речевой информации из защищаемых помещений. Схема пассивного акустоэлектромагнитного канала утечки акустической речевой информации. Схема активного акустоэлектромагнитного канала утечки акустической речевой информации. Средства перехвата акустической речевой информации, использующие эффект акустоэлектромагнитного преобразования речевого сигнала. Каналы утечки акустической речевой информации, использующие высокочастотные генераторы.	
Угрозы безопасности информации, связанные с НСД Понятие и общая классификация угроз безопасности информации, связанных с НСД. Источники угроз безопасности информации. Модели угроз безопасности информации, связанных с НСД. Методы выявления и анализа угроз безопасности информации, уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах. Банк данных угроз безопасности информации, включающий базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах. Описание уязвимостей программного обеспечения, включенных в базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах. Международный подход к выявлению и анализу уязвимостей, базы данных, содержащие уязвимости, в том числе CVE. Общая система оценки уязвимостей (стандарт CVSS).	16,2
Практика	16,2
Промежуточная аттестация	14,8
2-ой семестр	
Меры и средства защиты информации от НСД Общая характеристика и классификация мер и средств защиты информации от НСД. Требования к мерам защиты информации от НСД, реализуемым в автоматизированной (информационной) системе. Меры защиты информации от НСД. Средства защиты информации от НСД. Межсетевые экраны, требования к ним и способы применения. Системы обнаружения вторжений, требования к ним и способы применения. Средства антивирусной защиты, требования к ним и способы применения. Специальные программно-аппаратные и программные комплексы доверенной загрузки и разграничения контроля доступа. Средства регистрации и учета. Средства (механизмы) обеспечения целостности информации. Криптографические средства защиты информации. Перспективные технологии биометрической аутентификации. DLP-системы, их возможности и перспективы применения. Общий порядок разработки и производства средств защиты информации от НСД. Установка, настройка, эксплуатация и техническое обслуживание средств защиты информации от НСД. Мероприятия по физической защите объекта информатизации и отдельных технических средств, исключающих НСД к техническим средствам, их хищение и нарушение работоспособности.	12,2
Информация как объект защиты от специальных воздействий	20,2

Информация как объект защиты от специальных электромагнитных воздействий. Технические средства обработки информации как объекты защиты от специальных электромагнитных воздействий. Физические процессы, возникающие при воздействии мощными электрическими и магнитными полями и токами на технические средства обработки информации. Угрозы безопасности информации от специальных электромагнитных воздействий. Модели угроз. Механизм влияния электромагнитных и электрических воздействий на технические средства обработки информации. Меры и средства защиты информации от специальных воздействий. Принципы использования экранирующих и поглощающих свойств различных материалов для защиты информации от электромагнитных воздействий. Принципы использования фильтрующих и поглощающих устройств и материалов для защиты информации от электрических воздействий. Организация и содержание работ по защите информации от специальных воздействий, состав и содержание необходимых документов.	
Организация защиты конфиденциальной информации на объектах информатизации Организация работ по созданию и эксплуатации объектов информатизации и их систем защиты информации. Положение о порядке организации и проведения работ по защите конфиденциальной информации. Перечень сведений конфиденциального характера, подлежащих защите. Планирование работ по ТЗКИ. Сущность, цели и задачи планирования. Порядок разработки, согласования и утверждения планов проведения мероприятий по ТЗКИ. Реализация требований по защите акустической речевой конфиденциальной информации и информации, обрабатываемой в средствах вычислительной техники от утечки по техническим каналам. Реализация требований по защите информации от НСД и специальных воздействий на эксплуатируемом (функционирующем) объекте информатизации. Реализация требований по защите информации от НСД и специальных воздействий при создании нового объекта информатизации в защищенном исполнении. Особенности реализации требований по защите персональных данных. Создание и функционирование систем защиты конфиденциальной информации, как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий. Стадии и этапы создания систем защиты конфиденциальной информации. Порядок выполнения работ по защите информации о создаваемой автоматизированной системе в защищенном исполнении. Комплекс работ по созданию системы защиты информации (формирование требований к системе защиты информации; разработка (проектирование) системы защиты информации; внедрение системы защиты информации; аттестация объекта информатизации по требованиям безопасности информации и ввод его в действие; сопровождение системы защиты информации в ходе эксплуатации объекта информатизации). Разработка эксплуатационной документации на систему защиты информации.	20,2
Аттестация объектов информатизации по требованиям безопасности информации Организационно-правовые основы системы аттестации объектов информатизации по требованиям безопасности информации. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации (далее-система аттестации), как составной части единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Цели и виды аттестации объектов информатизации на соответствие требованиям безопасности информации. Участники аттестации и их полномочия(компетенции). Задачи, функции, права и обязанности органов по аттестации. Требования к органам по аттестации объектов информатизации. Деятельность аттестационных комиссий. Сводный реестр сертифицированной продукции, используемой в целях защиты информации на аттестованных объектах информатизации. Государственный контроль (надзор) за соблюдением порядка	6,2

аттестации и эксплуатацией аттестованных объектов информатизации. Основные мероприятия по проведению аттестации объектов информатизации на соответствие требованиям безопасности информации (подача и рассмотрение заявки на аттестацию объектов информатизации; предварительное ознакомление с аттестуемым объектом информатизации; разработка программ и методик аттестационных испытаний; проведение аттестационных испытаний объектов информатизации; оформление, регистрация и выдача аттестата соответствия). Требования к разработке, структуре, оформлению и утверждению программ и методик аттестационных испытаний объектов информатизации (требования к содержанию программ и методик аттестационных испытаний автоматизированных систем, защищаемых помещений). Требования обеспечения защиты конфиденциальной информации при проведении аттестации объектов информатизации. Методы проверки и испытаний, применяемые при проведении аттестационных испытаний (экспертно-документальный метод; измерение и оценка уровней ПЭМИН для отдельных технических средств автоматизированной системы и каналов утечки информации; проверка функций или комплекса функций защиты информации от НСД с помощью тестирующих средств, а также путем пробного пуска средств защиты информации от НСД и наблюдения за их выполнением; попытки «взлома систем защиты информации»). Разработка заключения и протоколов испытаний по результатам аттестации объектов информатизации. Оформление, регистрация и выдача «Аттестата соответствия». Порядок рассмотрения апелляций. Ввод в действие и эксплуатация аттестованных по требованиям безопасности информации объектов информатизации. Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объектов информатизации. Вывод из эксплуатации аттестованных по требованиям безопасности информации объектов информатизации.	
Контроль состояния технической защиты конфиденциальной информации Основные задачи контроля состояния ИБ. Классификация видов контроля состояния ИБ. Система документов по контролю состояния ИБ. Вопросы, подлежащие проверке при контроле состояния ИБ. Организационный и технический контроль состояния ИБ. Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН. Методы и средства контроля защищенности конфиденциальной акустической речевой информации от утечки по техническим каналам. Методы и средства контроля защищенности конфиденциальной информации от НСД. Документирование результатов контроля. Требования к средствам контроля защищенности конфиденциальной информации. Цели, задачи и функции мониторинга информационной безопасности средств и систем информатизации. Состав и структура системы мониторинга. Основные принципы системы мониторинга информационной безопасности средств и систем информатизации. Обнаружение и идентификация инцидентов безопасности информации, а также событий, приводящих к возникновению инцидентов. Анализ инцидентов безопасности информации, в том числе определение источников и причин возникновения инцидентов, а также оценку их последствий. Планирование мер по устранению инцидентов безопасности информации, в том числе по восстановлению систем информатизации, их сегментов и средств, входящих в их состав, в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов. Планирование мер по предотвращению повторного возникновения инцидентов безопасности информации. Контроль за событиями безопасности и действиями пользователей в средствах и системах информатизации. Контроль (анализ) защищенности информации, содержащейся в средствах и системах информатизации. Анализ и оценка	14,2

функционирования систем защиты информации систем информатизации, включая выявление, анализ и устранение недостатков в функционировании систем защиты информации систем информатизации. Периодический анализ изменения угроз безопасности информации в средствах и системах информатизации, возникающих в ходе их эксплуатации. Документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в средствах и системах информатизации. Разработку предложений (рекомендаций) по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) систем защиты информации систем информатизации, повторной оценке эффективности систем защиты информации систем информатизации или проведении дополнительных работ, по оценке эффективности систем защиты информации систем информатизации.	
Практика	32,2
Итоговая аттестация	38,8
Итого	252

Учебно-тематический план Программы определяет тематическое содержание, последовательность разделов и (или) тем и их трудоемкость (табл.6).

Таблица 6

		Часы				Контроль
№ п/п	Наименование раздела (модуля)	Лекции	Лабораторные работы	Практика	Самостоятельной работы	
	1-ый семестр					
1	Цели и задачи ИБ. Защищаемые информация и информационные ресурсы. Объекты защиты	1				0,1 Зачет
2	Определение угроз безопасности информации ограниченного доступа	1	2		2	0,1 Зачет
3	Основы нормативного правового обеспечения ИБ	2	2		2	0,2 Зачет
4	Средства и системы обработки информации	4	4		16	0,2 Зачет
5	Способы и средства технической защиты конфиденциальной информации от утечки по техническим каналам	4	4		16	0,2 Зачет
6	Угрозы безопасности информации, связанные с НСД	4	4		8	0,2 Зачет
7	Практика			16		0,2 Зачет
8	Промежуточная аттестация					14,8 Зачет

	2-ой семестр					
9	Меры и средства защиты информации от НСД	2	2		8	0,2 Зачет
10	Информация как объект защиты от специальных воздействий	4	4		12	0,2 Зачет
11	Организация защиты конфиденциальной информации на объектах информатизации	4	4		12	0,2 Зачет
12	Аттестация объектов информатизации по требованиям безопасности информации	2	2		2	0,2 Зачет
13	Контроль состояния технической защиты конфиденциальной информации	4	4		6	0,2 Зачет
14	Практика			32		0,2 Зачет
15	Итоговая аттестация			24		14,8 Зачет
	Зачет итоговый					
	ВСЕГО	32	32	72	84	32

X. ФОРМЫ АТЕСТАЦИИ

Слушатели, успешно выполнившие все элементы учебного плана, допускаются к промежуточной аттестации.

Промежуточная аттестация по Программе проводится в форме зачета.

Зачет проводится по итогам процедуры внешнего промежуточного ассессмента.

Итоговая аттестация проводится в форме процедуры внешнего ассессмента и защиты выпускной работы, связанной с решением практико-ориентированной задачи в составе проектной команды.

Лицам, успешно освоившим Программу (в области создания алгоритмов и программ, пригодных для практического применения, или навыков использования и освоения цифровых технологий, необходимых для выполнения нового вида профессиональной деятельности) и прошедшим итоговую аттестацию в рамках проекта «Цифровые кафедры», выдается документ о квалификации: диплом о профессиональной переподготовке.

При освоении ДПП ПП параллельно с получением высшего образования диплом о профессиональной переподготовке выдается не ранее получения соответствующего документа об образовании и о квалификации (за исключением лиц, имеющих среднее профессиональное или высшее образование).

XI. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Фонд оценочных средств (ФОС) представлен, в Приложении 1 к программе переподготовки.

XII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

Учебная аудитория для лекционных занятий оснащена универсальными техническими средствами обеспечения учебного процесса в составе:
мультимедийного персонального компьютера (ноутбука) (с приводом лазерных дисков типа DVD-RW, звуковым сопровождением и т.п.);
мультимедийного проектора с дистанционным управлением.
Учебная аудитория для практических и самостоятельных занятий оснащена мультимедийным персональным компьютером (ноутбуком) преподавателя (сервером) и пользовательскими терминалами по числу обучающихся, объединенных локальной сетью («компьютерный» класс).
Учебные аудитории и средства вычислительной техники аттестованы в установленном порядке.
Для изучения учебной дисциплины приобретены специализированные учебные лабораторные комплексы для проведения:
аттестационных испытаний объектов информатизации на соответствие требованиям по защите информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок;
аттестационных испытаний автоматизированных систем от НСД по требованиям безопасности информации
аттестационных испытаний и аттестация объектов информатизации на соответствие требованиям по защите информации от утечки акустической речевой информации.
Специализированные лаборатории оснащены полным комплексом контрольно-измерительного и испытательного оборудования, средствами контроля защищенности, тест-объектами, эквивалентами строительных и иных конструкций, позволяющих полностью имитировать реальные ситуации при выполнении аттестационных испытаний объектов информатизации.
Для проведения занятий требуются:
а) контрольно-измерительное и испытательное оборудование:
генераторы шумовых сигналов, вид шумового сигнала: «белый шум» (с нормальным распределением плотности вероятности мгновенных значений); хаотическая импульсная последовательность. Диапазон частот 175…5600 Гц;
низкочастотные генераторы сигналов, диапазон частот 175…5600 Гц, выходное напряжение не менее 5 В;
усилители мощности, диапазон частот 175…5600 Гц, выходная мощность не менее 10 Вт;
акустические излучатели, диапазон воспроизводимых частот 175…5600 Гц. Уровень звукового давления на расстоянии 1 м от излучателя в свободном поле не менее 95 дб. Неравномерность АЧХ не более ±6 дб;

измерители шума и вибраций (шумомеры), диапазон частот 175…5600 Гц, пределы измерения уровней сигналов 25-120 дБ, класс точности не ниже 2-го;
селективные микровольтметры, диапазон частот 175…5600 Гц, погрешность измерения не более ±15 %;
измерительные приемники (анализаторами спектра), диапазон измеряемых параметров 9 кГц – 1000 МГц, погрешность измерения не более 2 дб;
селективные нановольтметры, диапазон частот 175…5600 Гц, погрешность измерения не более ±15 %;
измерительные микрофоны, диапазон частот 175…5600 Гц, чувствительность не хуже 10 мВ/Па, неравномерность АЧХ не более ±1дБ;
измерительные антенны, диапазон измеряемых частот: по магнитной составляющей 9 кГц…30 МГц; по электрической составляющей 9 кГц… 1000 МГц, погрешность измерения не более ±2 дБ;
вибродатчики (акселерометры), диапазон частот 175…5600 Гц, чувствительность не хуже 1 мВ/мс-1, неравномерность АЧХ не более 10%;
измерительные пробники – диапазон измеряемых параметров 9кГц…300 МГц;
полосовые октавные фильтры со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц, диапазон частот 175…5600 Гц, номинальное ослабление в полосе пропускания фильтра 0 дБ, класс точности 1-й или 2-й, АЧХ в соответствии с ГОСТ 17168-82;
осциллографы, диапазон измеряемых параметров 0…5 МГц;
оптические тестеры (измерители мощности), длина волны калибровки, нм 850, 1310, 1550; диапазон измерений оптической мощности дБ, от 3 до минус 10-минус 73, разрешающая способность, дБ -0,1…0,001;
рефлектометры (микрорефлектометры), длина волны калибровки, нм 850, 1310, 1550; диапазон измерений оптической мощности дБ, от 3 до минус 26-минус 65, разрешение по затуханию, дБ - 0,001;
б) средства контроля защищенности:
программные средства формирования и контроля полномочий доступа в информационных (автоматизированных) системах (должны иметь сертификат соответствия ФСТЭК России);
средства контроля эффективности применения средств защиты информации (должны иметь сертификат соответствия ФСТЭК России);
программное средство контроля целостности программ и программных комплексов (должно иметь сертификат соответствия ФСТЭК России);
система контроля (анализа) защищенности информационных систем (должна иметь сертификат соответствия ФСТЭК России);
средства, предназначенные для осуществления тестирования на проникновение.

XIII. СПИСОК ЛИТЕРАТУРЫ

1. Белов Е.Б. Основы информационной безопасности: учеб. пособие / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.

2. Запечников С.В. Информационная безопасность открытых систем. Часть 1: учебник для вузов / С.В. Запечников, М.Г. Милославская, А.И. Толстой, Д.В.Ушаков. – М.: Горячая линия – Телеком, 2006. – 686 с.
3. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т.1. Технические каналы утечки информации. – М.: НПЦ «Аналитика»,2008. – 436 с.
4. Будников С.А., Паршин Н.В. Информационная безопасность автоматизированных систем: учеб. пособие. – 2-е изд., расширен. и дораб. Воронеж: ГУП ВО «Воронежская областная типография – издательство им. Е.А. Болховитинова», 2011. – 354 с.
5. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: учеб. пособие. – М.: ИТК «Дашков и К», 2006. – 336 с.
6. Кондратьев А.В. Организация и содержание работ по выявлению и оценке основных видов ТКУИ, защита информации от утечки: справочное пособие. – М.: МАСКОМ, 2011. – 256 с.
7. Некоторые вопросы защиты информации: методич. Пособие. – М.: НОВО, 2012 – 164 с.
8. Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации: учеб. пособие / В.С. Горбатов, С.В.Дворянкин, А.П. Дураковский, Р.С. Енгалычев [и др.]; под общ. Ред. Ю.Н. Лаврухина. – М: НИЯУ МИФИ, 2014. – 560 с.
9. Контроль защищенности информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок. Аттестационные испытания по требованиям безопасности информации: учеб. пособие / А.А. Голяков, В.С. Горбатов, А.П. Дураковский, А.Е. Панин, М.С. Чистяков; под общ. ред. Ю.Н. Лаврухина. – М: НИЯУ МИФИ, 2014. – 208 с.: ил.
10. Контроль защищенности речевой информации в помещениях. Аттестационные испытания выделенных помещений по требованиям безопасности информации: учеб. пособие / В.С. Горбатов, А.П. Дураковский, И.В. Куницын, А.Е. Панин; под общ. ред. Ю.Н. Лаврухина. – М: НИЯУ МИФИ, 2014. – 248 с.: ил.
11. Контроль защищенности речевой информации в помещениях. Аттестационные испытания вспомогательных технических средств и систем по требованиям безопасности информации: Учебное пособие / А.П. Дураковский, И.В.Куницын, Ю.Н. Лаврухин. – М: НИЯУ МИФИ, 2015. – 152 с.;
12. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: учеб. пособие. – М.: «Горячая линия – Телеком, 2005.
13. Снытников А.А. Лицензирование и сертификация в области защиты информации. – М.: Гелиос-АРВ, 2003.
14. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005.
15. Хорев А.А. Аттестация объектов информатизации и выделенных помещений // Специальная техника. – 2006. –№4.

16. Будников С.А., Паршин Н.В. Информационная безопасность автоматизированных систем: учеб. пособие, 2-е изд., доп. – Изд-во им. Е.А. Болховитинова», Воронеж, 2011.
17. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. №608.
18. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. №608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
19. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.
20. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
21. Специальные требования и рекомендации по защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
22. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден Гостехкомиссией России, 1992.
23. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден Гостехкомиссией России, 1992.
24. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.
25. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
26. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
27. ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России, 1998.
28. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
29. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
30. ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения. Росстандарт, 2012.

31. ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний. Росстандарт, 2013.
32. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
33. Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи (МД по ТЗИ ВОСП-К). Утвержден приказом ФСТЭК России 15 марта 2012г. № 27.
34. Временная методика оценки защищенности информации ограниченного доступа, обрабатываемой техническими средствами и системами с элементами беспроводных технологий, от утечки по каналу побочных электромагнитных излучений и наводок. Утверждена ФСТЭК России 21 декабря 2007 г.
35. Перечень технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденными постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 (новая редакция). Утвержден ФСТЭК России 4 апреля 2015 г

XIV. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ"

Базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

XV. ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1. Программно-аппаратный комплекс доверенной нагрузки – ПАК «Соболь»;
2. Сканер безопасности XSpider;
3. MaxPatrol SIEM;
4. Программа поиска и гарантированного уничтожения информации на дисках «TERRIER»;
5. Программа фиксации и контроля исходного состояния программного комплекса «ФИКС»;
6. Программное обеспечение «Средство создания модели системы разграничения доступа» «Ревизор-1XP»;
7. Программа контроля полномочий доступа к информационным ресурсам «Ревизор-2XP»;
8. Средство защиты информации от несанкционированного доступа (автономные варианты);
9. Средство защиты информации Secret Net Studio;
10. Средство защиты информации Secret Net 7;
11. Средство защиты информации Secret Net LSP;
12. Средство защиты информации TrustAccess;

13. Аппаратно-программный комплекс шифрования «Континент»;
14. Средство защиты информации от несанкционированного доступа DallasLock 8.0;
15. Средство защиты платформ виртуализации vGate;
16. Средство антивирусной защиты «Антивирус Касперского»;
17. Система обнаружений вторжений и межсетевой экран «Security Studio Endpoint; Protection: Personal Firewall, HIPS»;
18. ПО InfoWatch Traffic Monitor Enterprise Edition (50 ед.);
19. ViPNet Client и другие продукты компании ИнфоТеКС;
20. Средство Управление мобильными устройствами (MDM).

ПРИЛОЖЕНИЕ 1. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

МИНИСТЕРСТВО НАУКИ и ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УЧЕБНЫЙ ЦЕНТР ИП и ПК ВолгГТУ

«ЦИФРОВАЯ КАФЕДРА»

«УТВЕРЖДАЮ»
Первый проректор ВолгГТУ
_____ С.В. Кузьмин
«___» _____ 2022 г.

Фонд оценочных средств по программе профессиональной переподготовки “КИБЕРБЕЗОПАСНОСТЬ”

Волгоград 2022

Директор ИП и ПК В.В. Шеховцов

Директор УЦ « ЦК»,
д.т.н., профессор. каф. ВТ А.Г. Кравец

Разработчики программы:

Зам.директора ИПиПК А.А. Алпатов

Одобрена комиссией по ДО НМС ВолгГТУ
Протокол № 5 от « 29 » 06 2022 г.

I. КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ

№	Наименование компетенции	Наименование инструментов	Уровень владения компетенцией	Вопрос по компетенции (Задание)	Ответ А	Ответ Б	Ответ В	Ответ Г
1	ПК-4 Применяет программное обеспечение для защиты информации	Инструменты-Антивирусы, firewall, Dr.Web, Kaspersky и т.д	1	**Что такое компьютерный вирус?**	прикладная программа	программа, выполняющая на компьютере несанкционированные действия	системная программа	
2	ПК-4 Применяет программное обеспечение для защиты информации	Инструменты-Антивирусы, firewall, Dr.Web, Kaspersky и т.д	1	**Основные типы компьютерных вирусов:**	аппаратные, программные, загрузочные	программные, загрузочные, макровирусы	файловые, программные, макровирусы	
3	ПК-4 Применяет программное обеспечение для защиты информации	Инструменты-Антивирусы, firewall, Dr.Web, Kaspersky и т.д	1	**Этапы действия программного вируса:**	размножение, вирусная атака	запись в файл, размножение, уничтожение программы	запись в файл, размножение	
4	ПК-4 Применяет программное обеспечение для защиты информации	Инструменты-Антивирусы, firewall, Dr.Web, Kaspersky и т.д	1	**В чем заключается размножение программного вируса?**	программа-вирус один раз копируется в теле другой программы	вирусный код неоднократно копируется в теле другой программы		
5	ПК-4 Применяет программное обеспечение	Инструменты-Антивирусы, firewall, Dr.Web,	2	**Что называется, вирусной атакой?**	отключение компьютера в результате попадания	неоднократное копирование кода вируса в код программы	нарушение работы программы, уничтожение данных,	

	для защиты информации	Kaspersky и т.д			вируса		форматирование жесткого диска	
6	ПК-4 Применяет программное обеспечение для защиты информации	Инструменты-Антивирусы, firewall, Dr.Web, Kaspersky и т.д	2	**Какие существуют методы реализации антивирусной защиты?**	только программные	аппаратные и программные	программные и административные	
7	ПК-4 Применяет программное обеспечение для защиты информации	Инструменты-Антивирусы, firewall, Dr.Web, Kaspersky и т.д	2	**Какие существуют основные средства защиты данных?**	аппаратные средства	программные средства	резервное копирование наиболее ценных данных	
8	ПК-4 Применяет программное обеспечение для защиты информации	Инструменты-Антивирусы, firewall, Dr.Web, Kaspersky и т.д	2	**Какие существуют вспомогательные средства защиты?**	аппаратные средства	административные методы и антивирусные программы	программные средства	
9	ПК-4 Применяет программное обеспечение для защиты информации	Инструменты-Антивирусы, firewall, Dr.Web, Kaspersky и т.д	3	**На чем основано действие антивирусной программы?**	на ожидании начала вирусной атаки	на сравнении программных кодов с известными вирусами	на удалении зараженных файлов	
10	ПК-4 Применяет программное обеспечение для защиты информации	Инструменты-Антивирусы, firewall, Dr.Web, Kaspersky и т.д	3	**О каком вирусе идет речь? «Могут привести к сбою и зависанию при работе компьютера»**	загрузочный	файловый	опасный	
11	ПК-4	Инструменты-	3	**Этапы действия**	запись в файл,	размножение,	запись в файл,	

	Применяет программное обеспечение для защиты информации	Антивирусы, firewall, Dr.Web, Kaspersky и т.д		**программного вируса:**	размножение	вирусная атака	размножение, уничтожение	
12	ПК-4 Применяет программное обеспечение для защиты информации	Инструменты-Антивирусы, firewall, Dr.Web, Kaspersky и т.д	3	**На чем основано действие антивирусной программы?**	на удалении зараженных файлов	на сравнении программных кодов с известными вирусами	на ожидании начала вирусной атаки	

ФОС_Кибербезопасность

КЕЙС №1

В коммерческой организации, которая занимается поставками компьютерной техники для государственных и муниципальных органов. При сумме потенциального контракта (поставки) более 1 500 000 рублей данная компания должна участвовать в тендере, соответственно сталкиваться с конкурентной борьбой во время проведения торгов. Компания не имеет никаких внутренних документов, касающихся информационной безопасности, в том числе политики безопасности. В процессе участия в одной из процедур торгов ответственный менеджер по торгам получает на корпоративную почту письмо с заголовком "Срочно. Документы" с неизвестного адреса. Данное письмо содержит единственный архивный файл без текста самого письма. Менеджер открывает архив, после чего автоматически запускается вирус, который не только блокирует рабочий компьютер с установленным программным обеспечением для торгов и авторизированной электронной подписью организации, но и пытается распространяться по внутренней сети компании. Сотрудники ИТ-отдела реагируют достаточно оперативно, локализуют распространение вируса, устраняют сам вирус и последствия его действия на всех зараженных компьютерах в течение 3-х часов. Но за это время торги закрываются, и компания упускает крупный контракт.

Компетенция ПК-4 Применяет программное обеспечение для защиты информации	**Уровень сформированности компетенции**
Вопрос: Провести тестирование на проникновение (penetration test) для проверки уровня информационной безопасности инфраструктуры организации.	
Кто, по Вашему мнению, виноват в данной ситуации?	0
Кто должен инициировать создание и внедрение политики информационной безопасности в организации?	1
Зачем нужна политика информационной безопасности?	2
Ваши рекомендации по разработке политики ИБ.	3
Сделайте критический анализ политики ИБ какой-нибудь известной компании?	3

КЕЙС №2

В ноябре 1988 года случилась первая эпидемия, вызванная сетевым червем. На офисных компьютерах стояла операционная система Unix. Доступ в интернет имел один компьютер, остальные были связаны с ним по локальной сети. Это позволяло маскироваться под задачу легальных пользователей системы. Однако из-за ошибок в коде безвредная по замыслу программа неограниченно рассылала свои копии по другим компьютерам сети, запускала их на выполнение и таким образом забирала под себя все сетевые ресурсы. Червь Морриса заразил по разным оценкам от 6000 до 9000 компьютеров в США (включая Исследовательский центр NASA) и практически парализовал их работу сроком до пяти суток. Общие убытки были оценены в минимум 8 миллионов часов потери доступа и свыше миллиона часов прямых потерь на возобновление работоспособности систем. Общая стоимость этих расходов оценивается в 96 миллионов долларов.

Компетенция ПК-4 Применяет программное обеспечение для защиты информации	**Уровень сформированности компетенции**
Вопрос: Подбор и использование наиболее эффективных антивирусных приложений для профилактики и лечения ПО.	
Что делал Червь Морисса, какие действия необходимо предпринять, чтобы выявить причину заражения и как обезвредить?	0
С какими угрозами информационной безопасности можно столкнуться в наши дни и как их нейтрализовать?	1
Выберите 2-3 основных угрозы, охарактеризуйте их и обоснуйте их выбор.	2
Как избежать заражения вирусами и какую необходимо делать профилактику ПО?	3
Подбор и использование наиболее эффективных антивирусных приложений для профилактики и лечения ПО.	3

II.ВЫПУСКНАЯ РАБОТА

Выпускная работа связана с решением практико-ориентированной задачи, представленной предприятиями – партнерами, в составе проектной команды.

Тема выпускной работы может декомпозироваться на подзадачи, при этом четко очерчивается список всех работ каждого исполнителя проекта.

Отчет выпускной работы осуществляется в виде защиты на последней учебной неделе Программы.
Выпускная работа состоит в формировании концепции, архитектуры системы и реализации проекта для практико-ориентированной задачи в сферах кибербезопасности, защиты информации в информационных системах.
Содержание пояснительной записки к выпускной работе должно содержать:

1. Описание постановки практико-ориентированной задачи проекта.
2. Результаты исследования существующих разработок и применяемых методов решения задач по теме проекта.
3. Обоснование необходимости проведения исследований и разработки нового метода решения задачи.
4. Этические нормы, правовые аспекты и используемые стандарты в области кибербезопасности и смежных областей применяемые в проекте.
5. Архитектура системы кибербезопасности, возможная интеграция с внешними сервисами и реализация встраиваемой системы.
6. Обоснование выбранной архитектуры.
7. Календарный план реализации проекта с декомпозицией задач и учетом необходимых ресурсов.
8. Методы решения задач с обоснованием выбора.
9. Описание решения практико-ориентированной задачи и этапов ее реализации.
10. Описание процесса тестирования и результатов тестирования.

Примерные темы выпускных работ:

1. Реализация программных средств защиты информации в системе корпоративной мобильности
2. Организация системы кибербезопасности производственных систем
3. Организация защищенного web-соединения
4. Реализация системы инсталляции с лицензированием средствами Microsoft Visual Studio
5. Разработка программных средств защищенной аудио-видео трансляции
6. Реализация защиты от копирования экрана
7. Разработка программных средств контроля и блокирования устройств ввода-вывода ЭВМ