АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ВЫСШЕГО ОБРАЗОВАНИЯ
«УНИВЕРСИТЕТ ИННОПОЛИС»

УТВЕРЖДЕНА

Приказ № 286-ДО

от «22» июля 2022 г.

Дополнительная профессиональная программа
(программа профессиональной переподготовки)

Интернет вещей и машинное обучение
(наименование программы)

дополнительное профессиональное образование
(подвид дополнительного образования)

Иннополис 2022 г.

I. Общие положения

1. 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»; 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 11.03.02 Инфокоммуникационные технологии и системы связи (уровень бакалавриата), утвержденный приказом Минобрнауки России от «19» сентября 2017 г. № 930, (далее вместе – ФГОС ВО)), а также профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях», утвержден приказом Министерства труда и социальной защиты РФ от 03 ноября 2016 г №608н.

2. Профессиональная переподготовка заинтересованных лиц (далее – Слушатели), осуществляемая в соответствии с Программой (далее – Подготовка), имеющей отраслевую направленность[1] Информационно-коммуникационные технологии, проводится в ФГБОУ ВО Забайкальском государственном университете (далее – Университет) в соответствии с учебным планом в очной/заочной форме обучения[2].

3. 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

[1] Варианты отраслевой направленности: «Городское хозяйство»; «Финансовые услуги»; «Строительство»; «Добывающая промышленность»; «Обрабатывающая промышленность»; «Транспортная инфраструктура»; «Здравоохранение»; «Энергетическая инфраструктура»; «Образование»; «Сельское хозяйство и агропромышленный комплекс»; «Информационно-коммуникационные технологии»; «Искусство и культура»

[2] При реализации Программы допускается использовать сетевую форму обучения с организациями реального сектора экономики субъекта Российской Федерации

«Специалист по защите информации в телекоммуникационных системах и сетях».

4. Программа регламентирует требования к профессиональной переподготовке в области разработки инфокоммуникационных технологий и систем связи.

Срок освоения Программы составляет 504 академических часа.

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, не отнесенным к ИТ-сфере.

5. Область профессиональной деятельности – Информационно-коммуникационные технологии.

II. Цель

6. Целью подготовки слушателей по Программе является получение компетенции[3], необходимой для выполнения нового вида профессиональной деятельности в области информационных технологий и систем связи; приобретение новой квалификации в области обеспечения защиты средств связи сетей электросвязи (СССЭ) от несанкционированного доступа к ним (НСД) в условиях существования угроз их информационной безопасности (ИБ).

[3]Указать целевые группы обучающихся, определенные паспортом Федерального проекта: − обучающиеся по специальностям и направлениям подготовки, не отнесенным к ИТ-сфере, −обучающиеся по специальностям и направлениям подготовки ИТ-сферы (выбрать нужное)

III. Характеристика новой квалификации и связанных с ней видов профессиональной деятельности, трудовых функций и (или) уровней квалификации

7. Виды профессиональной деятельности, трудовая функция, указанные в профессиональном стандарте «Специалист по защите информации в телекоммуникационных системах и сетях» по соответствующей должности «Разработчик программного обеспечения» и «Специалист по компьютерным сетям», представлены в таблице 1:

Таблица 1

Характеристика новой квалификации, связанной с видом профессиональной деятельности и трудовыми функциями в соответствии с профессиональным стандартом «Специалист по защите информации в телекоммуникационных системах и сетях»

Область профессиональной деятельности	**Тип задач профессиональной деятельности**	**Код и наименование профессиональной компетенции**	**Трудовые действия**	**Трудовая функция**	**Обобщенная трудовая функция**	**Вид профессиональной деятельности**
Связь, информационные и коммуника-ционные технологии (в сфере разработки и функциониро-вания сетей электросвязи, средств и систем обеспечения защиты от НСД сетей электросвязи и циркулирующей в них информации)	Проектный, контрольно-аналитический, организационно-управленческий	ОПК-7.1. Способен формировать техническое задание и разрабатывать аппаратное и программное обеспечение компонентов защищенных телекоммуникационных систем. ОПК-7.2. Способен участвовать в разработке систем управления информационной безопасностью телекоммуникационных систем.	1.1. Выявление угроз НСД к сетям электросвязи. 1.2. Сбор и систематизация (анализ и оценка) сведений об угрозах НСД к сетям электросвязи. 1.3. Оценка уязвимостей сетей электросвязи с точки зрения возможности НСД к ним. 1.4. Выработка предложений по предотвращению и нейтрализации угроз НСД к сетям электросвязи. 2.1. Систематизация (анализ и оценка) сведений о методах, средствах и системах защиты СССЭ от НСД, принципах построения ЗТКС. 2.2. Формирование разделов технического задания на разработку средств и систем защиты СССЭ от НСД ЗТКС. 2.3. Проектирование элементов средств и систем защиты СССЭ от НСД ЗТКС. 2.4. Разработка предложенной и практическая реализация элементов, средств и систем защиты СССЭ от НСД ЗТКС,	1. Анализ угроз информационной безопасности в сетях электросвязи 2. Разработка средств и систем защиты СССЭ от НСД, защищенных телекоммуникационных систем	Разработка средств защиты СССЭ (за исключением сетей связи специального назначения) от НСД.	Разработка, обеспечение функционирования и менеджмент средств и систем обеспечения защиты средств связи сетей электросвязи от несанкционированного доступа к ним

			включая разработку программного обеспечения. 3.1. Формирование целей, приоритетов и ограничений системы защиты сети электросвязи от НСД, в том числе их изменение по мере изменения внешних условий и внутренних потребностей, включая требования уполномоченных федеральных органов исполнительной власти. 3.2.Анализ внутренних и внешних угроз НСД к сетям электросвязи. 3.3. Подготовка планов по развитию, модернизации системы защиты сети электросвязи от НСД, формирование требований к отдельным элементам и системе в целом. 3.4. Организация и контроль исполнения работ по развитию и модернизации систем защиты сетей электросвязи от НСД	3. Управление рисками систем защиты сетей электросвязи от НСД	Управление развитием средств и систем защиты от НСД	

Таблица 2

Характеристика новой и развиваемой цифровой компетенции в ИТ-сфере, связанной с уровнем формирования и развития в результате освоения Программы[4] «Кибербезопасность»

[4] На основании Модели цифровых компетенций, указанной в Приложении 2

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, рекомендованным и 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**
Защита информации	ПК -33. Применяет принципы защиты информации	Законодательство в области защиты информации (98, 152 и т.д. федеральные законы).	Не применяет принципы защиты информации	Участвует в проектах, применяющих принципы защиты информации, в составе команды под контролем опытных специалистов	Применяет самостоятельно принципы защиты информации в составе проектной команды	Применяет принципы защиты информации на уровне эксперта. Контролирует проекты, в которых применяются принципы защиты информации. Обучает других.
	ПК – 34. Применяет программное обеспечение для защиты информации	Антивирусы, firewall, Dr.Web, Kaspersky и т.д.	Не применяет программное обеспечение для защиты информации	Администрирует системы по защите информации. Настраивает и использует системы	Настраивает и использует программное обеспечение для защиты	Отвечает за эксплуатацию и разработку систем по защите информации

				под контролем опытных специалистов	информации самостоятельно	

IV. Характеристика новых и развиваемых цифровых компетенций, формирующихся в результате освоения программы

8. В ходе освоения Программы Слушателем приобретаются следующие профессиональные компетенции:

– ОПК-7.1. Способен формировать техническое задание и разрабатывать аппаратное и программное обеспечение компонентов защищенных телекоммуникационных систем;

– ОПК-7.2. Способен участвовать в разработке систем управления информационной безопасностью телекоммуникационных систем.

9. В ходе освоения Программы Слушателем совершенствуются следующие профессиональные компетенции:

– ПК-33. Применяет принципы защиты информации;

– ПК-34. Применяет программное обеспечение для защиты информации.

V. Планируемые результаты обучения по ДПП ПП

10. Результатами подготовки слушателей по Программе является получение компетенции, необходимой для выполнения нового вида профессиональной деятельности в области информационных технологий – Связь, информационные и коммуникационные технологии; приобретение новой квалификации в области обеспечения защиты средств связи сетей электросвязи (СССЭ) от несанкционированного доступа к ним (НСД) в условиях существования угроз их информационной безопасности (ИБ).

11. В результате освоения Программы слушатель должен:

Знать:

– объекты компьютерных технологий, используемые в обеспечении кибербезопасности;

– понятийный аппарат информационных технологий и особенности терминологии кибербезопасности;

– базовые составляющие в области развития систем информационной безопасности;

– технологии обнаружения компьютерных атак и их возможности;

– основные уязвимости и типовые атаки на современные компьютерные системы;

– основные принципы администрирования защищенных компьютерных систем;

– особенности реализации методов защиты информации современными программно-аппаратными средствами.

Уметь:

– ставить цели, формулировать задачи, связанные с обеспечением кибербезопасности;

– анализировать тенденции развития систем обеспечения кибербезопасности;

– применять знания о кибербезопасности в решении поставленных задач;

– применять механизмы защиты, реализованные в программно аппаратных комплексах, с целью построения защищенных компьютерных сетей;

– организовывать защиту сегментов компьютерной сети с использованием межсетевых экранов.

Иметь навыки:[5]

– применения современных технологий в области обеспечения кибербезопасности;

– проведения анализа в области обеспечения кибербезопасности.

– администрирования сетевых программно-аппаратных комплексов защиты информации;

– администрирования систем обнаружения компьютерных атак;

– средствами администрирования систем организации виртуальных частных сетей.

[5] Выделяются знания и умения в соответствии с профстандартом, связанные с результатами освоения Программы

VI. Организационно-педагогические условия реализации ДПП

12. Реализация Программы должна обеспечить получение компетенции, необходимой для выполнения нового вида профессиональной деятельности в области информационных технологий - Связь, информационные и коммуникационные технологии; приобретение новой квалификации в области обеспечения защиты средств связи сетей электросвязи (СССЭ) от несанкционированного доступа к ним (НСД) в условиях существования угроз их информационной безопасности (ИБ).

13. Учебный процесс организуется с применением[6] электронного обучения, инновационных технологий и методик обучения, способных обеспечить получение слушателями знаний, умений и навыков в области[7] связи, информационных и коммуникационных технологий (в сфере разработки и функционирования сетей электросвязи, средств и систем обеспечения защиты от НСД сетей электросвязи и циркулирующей в них информации).

14. Реализация Программы обеспечивается научно-педагогическими кадрами Университета, не менее 50% общего объема аудиторных или приравненных к ним часов в рамках ДПП ПП и следующими отвечающими критериям: 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,

[6] При необходимости указать нужное — электронного обучения, дистанционных образовательных технологий
[7] Разрабатывается на основе ФГОС ВО (3++), соответствует разделу 1.11 ФГОС ВО и конкретному профстандарту

привлечение работников организаций реального сектора экономики субъектов Российской Федерации.

VII. Учебный план ДПП

15. Объем Программы составляет 504 часа

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

Учебный план программы профессиональной переподготовки
«Кибербезопасность»

№ п/п	Наименование раздела (модуля)	Общая трудоемкость	Форма контроля
1.	Защита информационных ресурсов в компьютерных сетях	144	экзамен
2.	Техническая защита информации	72	зачет
3.	Государственная система защиты информации	72	зачет
4	Проектирование защищенных телекоммуникационных систем.	180	экзамен
	Промежуточная аттестация	24	
	Итоговая аттестация	12	Квалификационный экзамен
	Итого:	504	

VIII. Календарный учебный график

18. 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»

№ пп	Наименование раздела(модуля)	Учебные недели																				
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1.	Защита информационных ресурсов в компьютерных сетях	x	x	x	x	x	x																
2.	Техническая защита информации								x	x	x												
3.	Государственная система защиты информации.												x	x	x								
4.	Проектирование защищенных телекоммуникационных систем.																x	x	x	x	x	x	
5.	Промежуточная аттестация							x				x				x							x
6.	Итоговая аттестация																						x

IX. Рабочая программа учебных предметов, курсов, дисциплин (модулей)

19. Рабочая программа содержит перечень разделов и тем, а также рассматриваемых в них вопросов с учетом их трудоемкости.

Рабочая программа разрабатывается Университетом с учетом профессионального стандарта - Специалист по защите информации в телекоммуникационных системах и сетях.

№ п/п	Наименование и краткое содержание раздела(модуля)	Объем, часов
1.	*Защита информационных ресурсов в компьютерных сетях.* Основные темы: Компьютерные сети, информационно-аналитические системы и системы моделирования в технике. Киберпространство и основы кибербезопасности, векторы риска. Общие сведения о безопасности ПК и интернета, проблема интернет-зависимости. Методы обеспечения безопасности ПК и интернета, вирусы и антивирусы. Мошеннические действия в интернете, киберпреступления против личности, общества и государства, хакерские атаки и кибертерроризм. Технологии защищенной обработки информации.	144

2.	*Техническая защита информации.* Основные темы: Организация и проведение работ по технической защите информации в компьютерных сетях и системах. Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации. Технология межсетевого экранирования. Организация виртуальных частных сетей.	72
3.	*Государственная система защиты информации.* Основные темы: Концепция стратегии кибербезопасноти в РФ. Государственная политика в области кибербезопасности и государственный аудит. Вопросы кибербезопасности в современной государственной политике в области обеспечения национальной безопасности. Менеджмент кибербезопасности в национальном контексте, международные организации по кибербезопасности.	72
4.	*Проектирование защищенных телекоммуникационных систем.* Основные темы: Внутренние и внешние угрозы, связанные с новыми информационными технологиями. Управление ИТ-проектами и ИТ-процессами. Классификация ИТ-проектов, их место в деятельности компании. Жизненный цикл ИТ-проекта. Стандарты управления проектами и их применимость в сфере ИТ. Основы управления проектами и процессами в области информационных технологий. Вопросы проектирования и эксплуатации систем защиты информации.	180
5	**Промежуточная аттестация**	24
6	**Итоговая аттестация**	12

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

№ п/п	Наименование раздела(модуля)	Количество часов		
		аудиторных		самостоятельной работы (выполнение проектов и кейсов)
		Лекции	Семинары	
1.	Защита информационных ресурсов в компьютерных сетях	34	34	76
2.	Техническая защита информации	16	16	40
3.	Государственная система защиты информации	22	22	28
4.	Проектирование защищенных телекоммуникационных систем.	66	50	64

	Промежуточная аттестация	24
	Итоговая аттестация	12

X. Формы аттестации

21. Итоговая аттестация является обязательной для обучающихся, завершающих обучение по ДПП ПП. Итоговая аттестация проводится с участием представителей профильных организаций-работодателей, а также может проводиться в формате демонстрационного экзамена (в публичной форме).

В ходе итоговой аттестации обучающимися могут демонстрироваться презентации (защиты) разработанного цифрового решения (проекта), а также перечни решаемых ими проблем и эффектов, ожидаемых от их реализации (внедрения) в отрасль. Проектное решение должно отвечать критериям актуальности, законченности, а также возможности интеграции его компонентов в иные системы и сервисы.

Задачами проведения процедуры входной, промежуточной и итоговой оценки (ассесмента) являются:

1. Оценка уровня сформированности у обучающихся цифровых компетенций в области создания алгоритмов и программ, пригодных для практического применения, или навыков использования и освоения цифровых технологий, необходимых для выполнения нового вида профессиональной деятельности.

2. Оценка эффективности реализации ДПП ПП, обеспечивающих формирование цифровых компетенций в области создания алгоритмов и программ, пригодных для практического применения, или навыков использования и освоения цифровых технологий, необходимых для выполнения нового вида профессиональной деятельности.

Входная, промежуточная и итоговая оценка (ассесмент) обучающихся проводится на Платформе Университета Иннополис с

использованием двух инструментов: тестов и практических заданий в виде кейсов.

Итоговая оценка (ассесмент) проводится в дополнение к входной и промежуточной и не является итоговой аттестацией.

Обучающиеся не прошедшие процедуру оценки (ассесмента) в установленные сроки, могут быть допущены к итоговой аттестации и при успешном ее прохождении, получат диплом о переподготовке, но не будут засчитаны в показатель «Количество обученных в рамках проекта «Цифровые кафедры» параллельно с освоением основной образовательной программы высшего образования по программам профессиональной переподготовки, направленным на получение дополнительной квалификации по ИТ-профилю».

Текущий контроль результатов осуществляется преподавателем в процессе проведения теоретических и практических занятий, в форме контрольных работ, контрольных тестов, индивидуальных заданий и др. в целях получения информации:

- выполнении требуемых действий в процессе учебной деятельности;
- правильности выполнения требуемых действий;
- соответствии формы действия данному этапу усвоения учебного материала.

Промежуточная аттестация проводится по результатам освоения программ учебных дисциплин в форме дифференцированного зачета или экзамена на последнем занятии модуля. Формы и процедуры промежуточной аттестации по каждой дисциплине доводятся до сведения обучающихся перед началом учебного процесса.

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

Итоговая аттестация по Программе проводится в форме Квалификационного экзамена и в форме защиты итоговой аттестационной работы (индивидуального проекта).

22. 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).

23. Лицам, не прошедшим итоговую аттестацию или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть Программы и (или) отчисленным из Университета, выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому Университетом.

XI. Оценочные материалы

24. В качестве базовой технологии проведения процедуры входной, промежуточной и итоговой оценки (ассесмента) выбран метод ассесмент-центра. Ассесмент-центр – один из методов входной, промежуточной и итоговой оценки персонала, основанный на использовании взаимодополняющих методик, ориентированный на оценку профессиональных компетенций или отдельных умений и навыков, а также личностных характеристик человека, необходимых для решения конкретных задач. В ходе ассесмент-центра оценивается несколько заранее выбранных и описанных компетенций и/или личностных характеристик.

В целях обеспечения валидности методики при оценке кандидата

используется несколько инструментов входной, промежуточной и итоговой оценки (ассесмента). Входная, промежуточная и итоговая оценка (ассесмент) обучающихся проводится на Платформе Университета Иннополис с использованием двух инструментов: тестов и практических заданий в виде кейсов.

Контроль знаний, полученных слушателями при освоении разделов (модулей) Программы, осуществляется в следующих формах:

- текущий контроль успеваемости – обеспечивает оценивание хода освоения разделов Программы, проводится в форме устного опроса;

- промежуточная аттестация – завершает изучение отдельного модуля Программы, проводится в форме презентации проекта, зачета или экзамена;

- итоговая аттестация – завершает изучение всей программы.

При подготовке к сдаче теоретических вопросов итоговой аттестации, необходимо уделить терминологии, т.к. успешное овладение любой дисциплиной предполагает усвоение основных понятий, их признаков и особенности.

Подготовка к экзамену включает в себя:

- проработку основных вопросов модуля;
- чтение основной и дополнительной литературы по темам модуля;
- выполнение промежуточных и итоговых тестов;
- систематизацию и конкретизацию основных понятий дисциплины;
- составление примерного плана ответа на экзаменационные вопросы.

25. В ходе освоения Программы каждый слушатель выполняет следующие отчетные работы:

№ п/п	Наименование раздела (модуля)	Задание	Критерии оценки
1.	Защита информационных ресурсов в компьютерных сетях	Устный опрос (п.26.1)	«зачтено»: ответил на 80% вопросов «не зачтено»: правильные ответы составляют 1/3 часть от всех вопросов
2.	Техническая защита информации	Устный опрос (п.26.2)	«зачтено»: ответил на 80% вопросов «не зачтено»: правильные ответы составляют 1/3 часть от всех вопросов
3.	Государственная система защиты информации	Устный опрос (п.26.3)	«зачтено»: ответил на 80% вопросов «не зачтено»: правильные ответы составляют 1/3 часть от всех вопросов
4.	Проектирование защищенных телекоммуникационных систем.	Устный опрос (п.26.4).	«зачтено»: ответил на 80% вопросов «не зачтено»: правильные ответы составляют 1/3 часть от всех вопросов
5.	**Промежуточная аттестация**	Зачёт по теме модуля (п. 27.1, 27.2, 27.3, 27.4)	«зачтено»: ответил на 80% вопросов «не зачтено»: правильные ответы составляют 1/3 часть от всех вопросов
6.	**Итоговая аттестация**	Квалификационный экзамен Защита итоговой аттестационной работы (индивидуального проекта)	Уровень освоения программы, защита проекта, выполненного в рамках программы ДПО

26. Текущий контроль. Перечень примерных заданий

26.1. Модуль 1. «Защита информационных ресурсов в компьютерных сетях».

1. Тренды развития IT отрасли.
2. Проблемы безопасности инфраструктуры Интернета.
3. Понятие безопасности персонального компьютера.
4. Интернет и виды угроз компьютерной безопасности.
5. Стратегии снижения рисков. Аудит безопасности.
6. Мониторинг инцидентов кибербезопасности.
7. Кибератаки и техногенные катастрофы.
8. Защита IT-инфраструктур критически важных объектов.
9. Задачи и уровни обеспечения защиты киберпространства.
10. Основные аспекты кибербезопасности.

11. Атаки на протоколы и службы Интернет. Методы и средства защиты.
12. Аудит безопасности компьютерных систем. Цели, стандарты, подходы.
13. Конфигурирование сетевых фильтров на базе настроек безопасности протокола TCP/IP в ОС Windows XP.
14. Назначение систем обнаружения атак. Классификация систем обнаружения атак.

26.2. Модуль 2. «Техническая защита информации».

1. Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии.
2. Использование микрофона телефонного аппарата при положенной телефонной трубке.
3. Утечка информации по сотовым цепям связи.
4. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.
5. Прослушивание информации от радиотелефонов.
6. Прослушивание информации от работающей аппаратуры.
7. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок.
8. Системы защиты от утечки по электромагнитному каналу.
9. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.
10. Технические средства для уничтожения информации и носителей информации, порядок применения.
11. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.

26.3. Модуль 3. «Государственная система защиты информации».

1. Концепция стратегии кибербезопасноти в РФ.
2. Вопросы кибербезопасности в современной государственной политике в

области обеспечения национальной безопасности.

3. Кибербезопасность как основной фактор национальной и международной безопасности.
4. Общие принципы стратегии кибербезопасности.
5. Информационное противоборство в бизнесе и кибербезопаснсть.
6. Конфиденциальность информации. Угрозы конфиденциальной безопасности.
7. Кибербезопасность как основной фактор национальной и международной безопасности.
8. Общие принципы стратегии кибербезопасности.
9. Международные нормы по кибербезопасности.

26.4. Модуль 4. «Проектирование защищенных телекоммуникационных систем».

1. Атаки на протоколы и службы Интернет. Методы и средства защиты.
2. Понятие межсетевых экранов. Компоненты межсетевого экрана. Политика сетевой безопасности.
3. Критерии фильтрации пакетов. Основные схемы сетевой защиты на базе межсетевых экранов.
4. Создание защищенных сегментов сетей с использованием межсетевых экранов.
5. Защита рабочих станций с использованием персональных сетевых фильтров.
6. Организация VPN-сетей. Задачи, решаемые VPN. Туннелирование в VPN.
7. Электронные сертификаты. Понятие инфраструктуры открытых ключей.
8. Протоколы и средства организации VPN на сетевом уровне.
9. Назначение, область применения, аутентификация и шифрование данных в протоколах SKIP и IPSec.

27. Промежуточная аттестация. Перечень примерных теоретических вопросов.

27.1. Модуль 1. «Защита информационных ресурсов в компьютерных сетях».

1. Защитные механизмы. Контроль целостности информационных ресурсов.
2. Управление защитными механизмами. Архитектура Active Directory.
3. Доверительные отношения. Контроллеры домена для чтения.
4. Подразделения. Учетные записи пользователей и компьютеров.
5. Группы. Объекты групповой политики.
6. Управление локальными групповыми политиками в системе Windows Vista/7/2008.
7. Технология настроек групповой политики (Group Policy Preferences).
8. Новый формат шаблонов для групповых политик в Windows Vista/7/2008.
9. Идентификация.Именование субъектов и объектов.
10. Маркер доступа (Security Access Token). Нулевые сеансы в Windows.
11. Субъекты доступа. Проблемы идентификации.
12. Протоколы аутентификации, используемые в Windows.
13. Протокол Lan Manager (LM). Протокол NTLMv2.
14. Сравнение алгоритмов аутентификации.
15. Аутентификация при удаленном доступе: протоколы CHAP, MS-CHAP, MS-CHAPv.2, EAP.
16. Парольная политика. Повышение безопасности учетной записи администратора.
17. Обеспечение безопасности гостевой учетной записи. Обход аутентификации при физическом доступе к компьютеру.
18. Архитектура системы безопасности.
19. Регистрация пользователя вне домена. Локальная база данных учетных записей.

27.2. Модуль 2. «Техническая защита информации».

1. Концепция технической защиты информации.

2. Утечка информации по техническим каналам.
3. Основные принципы технической защиты информации.
4. Организационные основы технической защиты информации.
5. Технические средства добывания информации.
6. Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов.
7. Методы противодействия утечке и добыванию информации.
8. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок.
9. Этапы эксплуатации технических средств защиты информации.
10. Виды, содержание и порядок проведения технического обслуживания средств защиты информации.
11. Установка и настройка технических средств защиты информации.
12. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.
13. Организация ремонта технических средств защиты информации.
14. Проведение аттестации объектов информатизации.

27.3. Модуль 3. «Государственная система защиты информации».

1. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации.
2. Защита информации (ЗИ). Процесс ЗИ, обеспечение и обслуживание процесса ЗИ, управление процессом ЗИ, координация деятельности в области ЗИ.
3. Системы защиты информации. Государственная система ЗИ (ГСЗИ). Целевые (объектные) и функциональные подсистемы ЗИ.
4. Концепция построения системы законодательного регулирования общественных отношений в области обеспечения информационной безопасности.
5. Роль и место Конституции РФ, конституционных законов, Гражданского Уголовного кодексов, Кодекса об административных правонарушениях,

Кодекса законов о труде, других общих и специальных законов в области ЗИ.

6. Информация как объект гражданских прав. Виды информации, подлежащие защите в процессе обычного гражданского оборота.
7. Регламентация вопросов защиты служебной, коммерческой и банковской тайны, интеллектуальной собственности.
8. Использование электронно-цифровой подписи при совершении сделок.
9. Система защиты государственной тайны. Перечень сведений, составляющих государственную тайну.
10. Отнесение сведений к государственной тайне и их засекречивание. Рассекречивание сведений и их носителей. Распоряжение сведениями, составляющими государственную тайну.
11. Информационные ресурсы как объект защиты. Классификация информационных ресурсов.
12. Государственные и негосударственные информационные ресурсы.
13. Персональные данные. Пользование информационными ресурсами.

27.4. Модуль 4. «Проектирование защищенных телекоммуникационных систем».

1. Особенности современных информационных систем как объекта защиты информации.
2. Классификация угроз безопасности информации.
3. Классификация ИТ-проектов, их место в деятельности компании.
4. Жизненный цикл ИТ-проекта.
5. Организационно-технические мероприятия по защите информации.
6. Вопросы проектирования, внедрения и эксплуатации АС и их систем зашиты информации.
7. Понятие инцидентов ИБ. Нормативная база в сфере управления инцидентами ИБ.
8. Система управления инцидентами ИБ. Обработка событий и инцидентов ИБ.

9. Организация процесса обработки технических данных в рамках реагирования на инциденты ИБ.
10. Сбор и фиксация информации об инцидентах ИБ.
11. Обеспечение режима защиты информации персональных данных
12. Протоколы PPTP, SSL. Назначение, область применения, аутентификация и шифрование данных.
13. Преимущества технологии терминального доступа. Обеспечение безопасности.

28. Итоговая аттестация

Итоговая аттестация проходит в форме Квалификационного экзамена и защиты итоговой аттестационной работы (индивидуального проекта), предполагающего проверку знаний, умений и навыков, полученных в результате изучения Программы.

Примерные темы итоговой аттестационной работы.

1. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Применение фильтрующего маршрутизатора WinRoute.
2. Защита сетевого трафика с использованием протокола IPSec в Windows NT 5.0. Организация VPN средствами протокола PPTP .
3. Применение специализированных средств организации VPN на примере «VipNet» и «StrongNET».
4. Применение COA Snort для обнаружения скрытого сканирования, атак, использующих преднамеренное нарушение структуры сетевых пакетов, атак вида «отказ в обслуживании».
5. Применение программных средств аудита информационной безопасности с целью тестирования состояния защищенности компьютерных систем от несанкционированного доступа и выработки мер защиты от выявленных угроз.
6. Криптографическое закрытие хранимых и передаваемых по каналам

данных. Active Directory и система безопасности. Новые возможности Active Directory в Windows Server 2008 R2.

7. Изменения в маркерах безопасности в Windows Vista и выше. Использование ключа реестра RestrictAnonymous в Windows 2000/XP/2003.
8. Протоколы аутентификации, используемые в Windows. Протокол Lan Manager (LM). Протокол NTLMv2. Сравнение алгоритмов аутентификации.
9. Шлюзы прикладного уровня. Сервер SQUID, принципы работы, варианты конфигурации. Контроль HTTP-трафика и электронной почты. Написание правил фильтрации, возможности по анализу содержимого.
10. Организация VPN средствами СЗИ «StrongNet». Описание системы. Генерация и распространение ключевой информации. Настройка СЗИ защищенного соединения.
11. Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ КриптоПро CSP. Защищенный обмен электронной почтой.
12. Применение технологии терминального доступа. Общие сведения о технологии терминального доступа. Обеспечение безопасности сервера ОС Windows Server 2003. Настройка сервера MSTS. Настройка протокола RDP.
13. Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.

XII. Материально-техническое и учебно-методическое обеспечение Программы

№ п\п	Наименование дисциплины (модуля), практик в соответствии с учебным планом	Наименование учебных кабинетов, лабораторий, мастерских и других помещений для реализации образовательной программы	Оснащенность учебных кабинетов, лабораторий, мастерских и других помещений для реализации образовательной программы
1.	Защита информационных ресурсов в компьютерных сетях	**Лаборатория программно-аппаратных средств обеспечения защиты информации. Учебная аудитория для проведения занятий практического и лабораторного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.** 672000, Россия, Забайкальский край, г.Чита, Центральный административный район, ул. Кастринская, д. 1, Корп 1. 08-211 **Учебная аудитория** 672000, Россия, Забайкальский край, г.Чита, Центральный административный район, ул. Кастринская, д. 1, Корп 1. 08-206	Рабочие места с антивирусными программными комплексами и аппаратными средствами аутентификации пользователя. Специализированное оборудование по защите информации от утечки по акустическому, акустоэлектрическому каналам, каналу побочных электромагнитных излучений и наводок, технические средства контроля эффективности защиты информации от утечки по указанным каналам. Оборудование криптозащиты – HW-100, АРМ VipNet клиент (12 лицензий) учебная защищенная сеть. Мультимедийный к-т в составе: переносной экран на треноге, мультимедийный проектор, ноутбук. Комплект специальной учебной мебели. Доска маркерная. Доступ к сети Интернет и обеспечение доступа в электронную информационно-образовательную среду организации Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования (выполнения курсовых работ), научно-исследовательской работы, самостоятельной работы. Комплект специальной учебной мебели: стол преподавателя; ученические столы; учебная доска аудиторная. Не закрепленный за конкретной учебной аудиторией комплект видеотехники переносной: ноутбук, колонки.

2.	Техническая защита информации	**Лаборатория технической защиты информации. Учебная аудитории для проведения занятий практического и лабораторного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.** 672000, Россия, Забайкальский край, г.Чита, Центральный административный район, ул. Кастринская, д. 1, Корп 1. Ауд. 08-202в **Учебная аудитория** 672000, Россия, Забайкальский край, г.Чита, Центральный административный район, ул. Кастринская, д. 1, Корп 1. Ауд. 08-206	Комплект специализированной учебной мебели. Доска маркерная. Наборы демонстрационного оборудования и учебно-наглядных пособий по дисциплинам, переносной мультимедийный к-т в составе: экран на треноге, мультимедийный проектор, ноутбук. Оборудование по защите информации от утечки: по акустическому, акустоэлектрическому каналам - AMTASTAMF004 измерители уровня шума 30-130dBA SmartSensorAR814, каналу побочных электромагнитных излучений и наводок, технические средства контроля эффективности защиты информации от утечки по указанным каналам. Лабораторный комплекс по электроакустике, измерители электромагнитного поля Benetech GM3120, Цифровой осциллограф Hantek, передатчики спортивной радиопеленгации ЛИСА-ПДАСР 3,5/144. Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования (выполнения курсовых работ), научно-исследовательской работы, самостоятельной работы. Комплект специальной учебной мебели: стол преподавателя; ученические столы; учебная доска аудиторная. Не закрепленный за конкретной учебной аудиторией комплект видеотехники переносной: ноутбук, колонки.
3.	Государственная система защиты информации	**Лаборатория сетей и систем передачи информации. Учебная аудитория для проведения занятий практического и лабораторного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.** 672000, Россия, Забайкальский край, г.Чита, Центральный	Рабочие места на базе вычислительной техники (ПК-15 шт.). Стенды сетей передачи информации с коммутацией пакетов и коммутацией каналов, структурированная кабельная система, телекоммуникационное оборудование, обучающее программное обеспечение, эмулятор активного сетевого оборудования, специализированное программное обеспечение для настройки телекоммуникационного оборудования. Комплект специальной учебной мебели. Доска маркерная. Рабочее место студента в составе

		административный район, ул. Кастринская, д. 1, Корп 1. Ауд. 08-215	АРМ оператора стерминальным доступом к ЭАТС «Сигма-СПб» и МС 240, телефонных аппаратов GE 2-9152.Комплект специализированной учебной мебели. Переносной мультимедийный к-т в составе: экран на треноге, мультимедийный проектор, ноутбук. 20 компьютеров обучающихся и 1 компьютер преподавателя (аппаратное обеспечение: сетевая плата, процессор AMD Ryzen 5, оперативная память объемом 8 Гб; HD 500 Gb. программное обеспечение: операционные системы Windows, UNIX, пакет офисных программ,) Технические средства обучения: компьютеры с лицензионным программным обеспечением, мультимедийная доска, программное обеспечение общего и профессионального назначения. Не закрепленный за конкретной учебной аудиторией комплект мультимедийной техники переносной: ноутбук, проектор, колонки. Лицензионное программное обеспечение: ABBYY FineReader (договор № 223-799 от 30.12.2014 (срок действия - бессрочно), ESET NOD32 Smart Security Business Edition (Договор № 223-1/19-ЗК от 24.09.2019 г. (продление) (срок действия – октябрь 2022г.), MS Office Standart 2013 (Договор № 223-799 от 30.12.2014 (срок действия - бессрочно), АИБС "МегаПро" (Договор №13215/223П/15-569 от 18.12.2015 (срок действия - бессрочно), MS Windows 7 (Договор № 223П/18-1 от 13.02.2018 (срок действия - бессрочно). Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования (выполнения курсовых работ), научно-исследовательской работы, самостоятельной работы. Комплект специальной учебной мебели: шкафы для литературы; стол преподавателя; ученические столы; учебная доска аудиторная. Не закрепленный за конкретной учебной аудиторией комплект видеотехники переносной: ноутбук, колонки. Доступ к сети Интернет и обеспечение доступа в электронную информационно-образовательную среду вуза.

		Учебная аудитория 672000, Россия, Забайкальский край, г.Чита, Центральный административный район, ул. Кастринская, д. 1, Корп 1. Ауд. 08-206	Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования (выполнения курсовых работ), научно-исследовательской работы, самостоятельной работы. Комплект специальной учебной мебели: шкафы для литературы; стол преподавателя; ученические столы; учебная доска аудиторная. Не закрепленный за конкретной учебной аудиторией комплект видеотехники переносной: ноутбук, колонки. Доступ к сети Интернет и обеспечение доступа в электронную информационно-образовательную среду вуза. Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования (выполнения курсовых работ), научно-исследовательской работы, самостоятельной работы. Комплект специальной учебной мебели: стол преподавателя; ученические столы; учебная доска аудиторная. Не закрепленный за конкретной учебной аудиторией комплект видеотехники переносной: ноутбук, колонки.
4.	Проектирование защищенных телекоммуникационных систем.	**Лаборатория программно-аппаратных средств обеспечения защиты информации. Учебная аудитория для проведения занятий практического и лабораторного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.** 672000, Россия,	Рабочие места с антивирусными программными комплексами и аппаратными средствами аутентификации пользователя. Специализированное оборудование по защите информации от утечки по акустическому, акустоэлектрическому каналам, каналу побочных электромагнитных излучений и наводок, технические средства контроля эффективности защиты информации от утечки по указанным каналам. Оборудование криптозащиты – HW-100, АРМ VipNet клиент (12 лицензий) учебная защищенная сеть. Мультимедийный к-т в составе: переносной экран на треноге, мультимедийный проектор, ноутбук. Комплект специальной учебной мебели. Доска маркерная. Доступ к сети Интернет и

		Забайкальский край, г.Чита, Центральный административный район, ул. Кастринская, д. 1, Корп 1. 08-211 **Учебная аудитория** 672000, Россия, Забайкальский край, г.Чита, Центральный административный район, ул. Кастринская, д. 1, Корп 1. 08-206	обеспечение доступа в электронную информационно-образовательную среду организации Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования (выполнения курсовых работ), научно-исследовательской работы, самостоятельной работы. Комплект специальной учебной мебели: стол преподавателя; ученические столы; учебная доска аудиторная. Не закрепленный за конкретной учебной аудиторией комплект видеотехники переносной: ноутбук, колонки.
	Промежуточная аттестация	**Кабинет Интернет-технологий. Лаборатория мультисервисных сетей. Учебная аудитория для проведения занятий практического и лабораторного типа, курсового и дипломного проектирования, научно-исследовательской работы, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы обучающихся.** 672000, Россия, Забайкальский край, г.Чита, Центральный административный район, ул. Кастринская, д. 1, Корп 1. Ауд. 08-204	Рабочие места на базе вычислительной техники и абонентские устройства, подключенные к сети «Интернет» с использованием проводных и беспроводных технологий, с установленным офисным пакетом и набором необходимых для проведения исследований дополнительных аппаратных и программных средств, а также оборудованием для печати. Обеспечение доступа в электронную информационно-образовательную среду организации. Переносной мультимедийный к-т в составе: экран на треноге, мультимедиапроектор, ноутбук. Комплект специальной учебной мебели. Стойка Hyperline, ASCON EnergySustems, ЦАТС МС 240 Зав.№403 Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования (выполнения курсовых работ), научно-исследовательской работы, самостоятельной работы. Комплект специальной учебной мебели: шкафы для литературы; стол преподавателя; ученические столы; учебная доска аудиторная.

		Учебная аудитория 672000, Россия, Забайкальский край, г.Чита, Центральный административный район, ул. Кастринская, д. 1, Корп 1. Ауд. 08-206	Не закрепленный за конкретной учебной аудиторией комплект видеотехники переносной: ноутбук, колонки. Доступ к сети Интернет и обеспечение доступа в электронную информационно-образовательную среду вуза. Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования (выполнения курсовых работ), научно-исследовательской работы, самостоятельной работы. Комплект специальной учебной мебели: стол преподавателя; ученические столы; учебная доска аудиторная. Не закрепленный за конкретной учебной аудиторией комплект видеотехники переносной: ноутбук, колонки.
	Итоговая аттестация	**Кабинет Интернет-технологий. Лаборатория мультисервисных сетей. Учебная аудитория для проведения занятий практического и лабораторного типа, курсового и дипломного проектирования, научно-исследовательской работы, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы обучающихся.** 672000, Россия, Забайкальский край, г.Чита, Центральный административный район, ул. Кастринская, д. 1, Корп 1. Ауд. 08-204	Рабочие места на базе вычислительной техники и абонентские устройства, подключенные к сети «Интернет» с использованием проводных и беспроводных технологий, с установленным офисным пакетом и набором необходимых для проведения исследований дополнительных аппаратных и программных средств, а также оборудованием для печати. Обеспечение доступа в электронную информационно-образовательную среду организации. Переносной мультимедийный к-т в составе: экран на треноге, мультимедиапроектор, ноутбук. Комплект специальной учебной мебели. Стойка Hyperline, ASCON EnergySustems, ЦАТС МС 240 Зав.№403 Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования (выполнения курсовых работ), научно-исследовательской работы, самостоятельной работы. Комплект специальной учебной мебели: шкафы для литературы; стол преподавателя; ученические столы; учебная доска аудиторная.

		Учебная аудитория 672000, Россия, Забайкальский край, г.Чита, Центральный административный район, ул. Кастринская, д. 1, Корп 1. Ауд. 08-206	Не закрепленный за конкретной учебной аудиторией комплект видеотехники переносной: ноутбук, колонки. Доступ к сети Интернет и обеспечение доступа в электронную информационно-образовательную среду вуза. Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования (выполнения курсовых работ), научно-исследовательской работы, самостоятельной работы. Комплект специальной учебной мебели: стол преподавателя; ученические столы; учебная доска аудиторная. Не закрепленный за конкретной учебной аудиторией комплект видеотехники переносной: ноутбук, колонки.

Учебно-методическое обеспечение Программы включает:

1. Рабочие программы модулей
2. Комплект теоретических материалов для освоения Программы.
3. Комплект мультимедийных материалов для освоения Программы.
4. Комплект оценочных материалов для контроля знаний, проверки умений и навыков.

XIII. Список литературы

Печатные издания

1. Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032. Вопросы кибербезопасности № 1(12) 2014. С. 28-35
2. Петренко С. А., Смирнов М. Б. Безопасность АСУТП и критической информационной инфраструктуры // СПб.: ООО «ИД «Афина». – 2018. ISBN 978-5-9909868-1-7. Учебно-методическое пособие [Электронная версия].
3. Куприяновский В.П. Кибер-физические системы как основа цифровой экономики / В.П. Куприяновский, Д.Е. Намиот, С.А. Синягов // International Journal of Open Information Technologies. – 2016. – Т.4 – №2. – С. 18-25.
4. Васильева Т.В. «Интернет Вещей» – стратегическое направление инновационных преобразований в экономике России / Т.В. Васильева // Вопросы современной науки и практики. Университет им. В.И. Вернадского. – 2013. – № 2 (46). – С. 187-193.
5. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2017.
6. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2 Организационное обеспечение информационной безопасности: учеб. пособие – М.: МИЭТ, 2016.
7. Чеботарева Анна Александровна. Информационное право : учеб. пособие.

- Чита : ЗабГУ, 2012. - 202 с. - ISBN 978-5-9293-0784-3 : 143-00.
8. Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей : учеб. пособие / под ред. В.Н. Гордиенко, М.С. Тверецкого. - Москва : Горячая линия-Телеком, 2008. - 392 с. : ил. - ISBN 978-5-9912-0010-3 : 345-00.

Электронные ресурсы

1. Внуков, Андрей Анатольевич. Защита информации : Учебное пособие / Внуков А.А. - 2-е изд. - М. : Издательство Юрайт, 2017. - 261. - (Бакалавр и магистр. Академический курс). - ISBN 978-5-534-01678-9 : 78.62.
2. Щеглов, Андрей Юрьевич. Защита информации: основы теории : Учебник / Щеглов А.Ю., Щеглов К.А. - М. : Издательство Юрайт, 2017. - 309. - (Бакалавр и магистр. Академический курс). - ISBN 978-5-534-04732-5 : 1000.00.
3. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Рекомендовано Государственным образовательным учреждением высшего профессионального образования "Академия Федеральной службы безопасности Российской Федерации" в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям направления подготовки 090300 - "Информационная безопасность вычислительных, автоматизированных и телекоммуникационных систем" и направлению подготовки 090900 - "Информационная безопасность". Регистрационный номер рецензии № 742 от 25 февраля 2010 г. (ГОУВПО "Московский государственный университет печати") /Девянин П.Н. - Moscow : Горячая линия - Телеком, 2012. - . - Модели безопасности компьютерных систем. Управление доступом и информационными потоками
[Электронный ресурс] : Учебное пособие для вузов / Девянин П.Н. - М. : Горячая линия - Телеком, 2012. -

http://www.studentlibrary.ru/book/ISBN9785991201476.html. – ISBN 978-5-9912-0147-6.

4. Полякова Татьяна Анатольевна. Организационное и правовое обеспечение информационной безопасности : Учебник и практикум / Полякова Т.А. - Отв. ред., Стрельцов А.А. - Отв. ред. - М. : Издательство Юрайт, 2017. - 325. - (Бакалавр и магистр. Академический курс). - ISBN 978-5-534-03600-8: 125.31.