МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

Институт дополнительного профессионального образования
и кадрового инжиниринга «Горизонт»

УТВЕРЖДАЮ
Председатель ученого совета,
И.о. ректора ФГБОУ ВО «МГТУ им. Г.И. Носова»
_____ Д.В. Терентьев
«25» января 2023 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

профессиональной переподготовки

Нейропсихология

Программа утверждена ученым советом МГТУ
Протокол № 2 «25» января 2023 г.

г. Магнитогорск, 2023

1 ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ (АННОТАЦИЯ)

1.1 Цель реализации программы

Цель программы: получение компетенций для выполнения нового вида профессиональной деятельности в сфере цифровой экономики в условиях нарастающих угроз безопасности информации, а именно, обеспечение безопасности информации в автоматизированных и информационных системах, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите.

Программа реализуется на русском языке.

1.2 Характеристика нового вида профессиональной деятельности и (или) присваиваемой квалификации

а) Область профессиональной деятельности:

Связь, информационные и коммуникационные технологии

б) Объекты профессиональной деятельности:

– информационные системы и технологии обработки информации для решения задач профессиональной деятельности;

– организационная деятельность по защите конфиденциальной информации;

– контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (СЗИ).

в) Виды и задачи профессиональной деятельности

Основные виды профессиональной деятельности:

– обеспечение безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями;

– определение информационных ресурсов, подлежащих защите, угроз безопасности информации и возможных путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объектов защиты;

Задачи профессиональной деятельности:

– проектирование сетевой корпоративной информационной инфраструктуры в защищенном исполнении,

– защита конфиденциальных данных в различных системах,

– защита персональных данных,

– определение типичных ошибок обеспечения информационной безопасности и формирования безопасной экосистемы организации.

г) Достижение 6 уровня квалификации в соответствии с профессиональным стандартом «Специалист по защите информации в автоматизированных системах».

1.3 Требования к результатам освоения программы

Программа разработана:

с учетом требований профессионального стандарта: проф. стандарт «Специалист по защите информации в автоматизированных системах», от 15.09.2016 № 522н;

ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата).

квалификационных требований: нац. программа «Цифровая экономика РФ», распоряжение от 28 июля 2017 г. № 1632-р; фед. проект «Кадры для цифровой экономики», протокол №6 от 27 декабря 2018 г.

Планируемые результаты обучения

По окончании обучения планируется достижение слушателями следующих результатов по реализации обобщенных трудовых функции:

– обслуживание систем защиты информации в автоматизированных системах (5 уровень квалификации);

– внедрение систем защиты информации автоматизированных систем (6 уровень квалификации);

В результате освоения программы у слушателей должны быть сформированы следующие **компетенции**:

– способность использовать языки программирования, информационные системы и технологии обработки информации для решения задач профессиональной деятельности;

– способность применять знания в области технологий связи и передачи данных при проектировании сетевой корпоративной информационной инфраструктуры в защищенном исполнении;

– системное и критическое мышление в цифровой среде.

– способность оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

– способность оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями.

– способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объектов защиты.

– способность администрировать операционные системы и вычислительные сети.

– способность проводить контрольные проверки работоспособности применяемых программных и программно-аппаратных СЗИ.

Трудовые действия:

- обеспечение защиты информации при выводе из эксплуатации автоматизированных систем;
- аудит защищенности информации в автоматизированных системах;
- установка и настройка СЗИ в автоматизированных системах;

Необходимые умения:

– реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования;

– оценивать информацию, подлежащую защите;

– осуществлять поиск новой методической документации по регламентации мероприятий и оказанию услуг в области защиты информации;

– применять действующую нормативную базу при обеспечении безопасности сетей ЭВМ;

– применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;

– проводить комплексное тестирование и отладку программных систем;

– работать с интегрированной средой разработки программного обеспечения;

– использовать шаблоны классов и средства макрообработки;

– использовать динамически подключаемые библиотеки;

– проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения;

– проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования;

– эффективно использовать полученную информацию для создания новых программных решений сложных задач в условиях неопределенности;

– осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области программных и программно-аппаратных СЗИ и систем с применением современных информационных технологий;

– передавать информацию с помощью цифровых средств.

– анализировать статистику реализации различных видов угроз;

– оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
– пользоваться банком угроз ФСТЭК России;
– разрабатывать проекты нормативных и организационно - распорядительных документов, регламентирующих работу по защите информации;
– определять основные угрозы безопасности в сетях ЭВМ;
– настраивать сетевое оборудование.

Необходимые знания:
– общие принципы построения современных языков программирования высокого уровня;
– современные стандарты информационного взаимодействия систем;
– алгоритмы анализа информационного пространства;
– виды тайн, подлежащие защите;
– основы законодательства РФ в области информационной безопасности.
– классификацию современных программных и программно-аппаратных СЗИ;
– состав, назначение функциональных компонентов и программного обеспечения программных и программно-аппаратных СЗИ;
– типовые структуры и принципы организации программных и программно-аппаратных СЗИ;
– основы цифровой гигиены;
– отличия законодательства РФ и других стран в сфере кибербезопасности;
– способы оформления документации по регламентации мероприятий и оказанию услуг в области защиты информации;
– типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях;
– характерные уязвимости, присущие каналами связи сетей ЭВМ при передаче информации по ним;
– организационные меры по защите информации;
– основные методики противодействия перехвату и несанкционированному съему информации при ее передаче по каналам связи сетей ЭВМ;
– классификацию и основные принципы действия оборудования и ПО, предназначенного для организации защищенных каналов передачи информации;
– особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах.

1.4. Категория слушателей

К освоению программы допускаются лица, имеющие высшее образование.

1.5 Требования к уровню подготовки поступающего на обучение и специальные требования (при наличии)

Для прохождения образовательной программы необходимо наличие у поступающего персонального компьютера и следующего программного обеспечения (ПО):

- Яндекс.Браузер, Веб-браузер Google Chrome или аналогичное ПО;
- Visual Studio Community или Visual Studio Code или аналогичное ПО для создания приложений на языке программирования C#;
- Microsoft Office или LibreOffice или аналогичное офисное ПО;
- Пакет OpenSSL.

Основные предъявляемые требования: умение работать с браузером, способность самостоятельно устанавливать и настраивать программное обеспечение на персональном

компьютере (ПК), разворачивать виртуальные машины, а также иметь представление об устройсте ПК и его функциональных возможностях.

Поступающий на обучение должен обладать знаниями по следующим темам: основы сети и системы передачи информации, организация ЭВМ, понимание концепций блокчейн и криптовалют, защита персональных данных, информационные системы и системы обработки данных, основы программирования.

Подтверждение уровня подготовки поступающего на обучение определяется в соответствии с требованиями пункта 3.1. настоящей программы.

1.6. Форма обучения

Очно-заочная с применением дистанционных образовательных технологий и электронного обучения.

1.7. Трудоемкость программы составляет 504 часа.

1.8. Выдаваемый документ

Лицам, успешно освоившим образовательную программу и успешно прошедшим итоговую аттестацию, выдается диплом о профессиональной переподготовке.

2 СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

	Наименование дисциплины (модуля)	Трудоемкость, ауд. час.	Всего, ауд. час.	Аудиторные занятия, час.		СРС, час.	Промежут очная аттестация	
				лекции	прак. занятия		Зач.	Экз
1.	Средства и системы обработки информации	100	8	3	5	92	1	
2.	Безопасность сетей ЭВМ	146	8	3	5	138		1
3.	Организационно-правовые основы технической защиты конфиденциальной информации	150	8	3	5	142		1
4.	Организация защиты конфиденциальной информации на ОИ	100	8	2	6	92	1	
5.	Итоговая аттестация	8				8		1
6.	ИТОГО	504	32	11	21	472		

2.2 Календарный учебный график

Наименование модуля/раздела/дисциплины/темы	Объем нагрузки для слушателя, ч.	Учебные месяцы					
		1 месяц	2 месяц	3 месяц	4 месяц	5 месяц	6 месяц
Средства и системы обработки информации	100						
Безопасность сетей ЭВМ	146						
Организационно-правовые основы технической защиты конфиденциальной информации	150						
Организация защиты конфиденциальной информации на ОИ	100						
Итоговая аттестация	8						

ИТОГО:	504						

Учебный график может корректироваться в соответствии с запросом заказчика.

Календарный учебный график составляется в форме расписания занятий при наборе группы.

2.3 Рабочие программы модулей.

Модуль 1. Средства и системы обработки информации

Цель освоения модуля

Целью освоения модуля является формирование профессиональных компетенций специалиста в области разработки пользовательских приложений на языке C# и проектирования сетевой корпоративной информационной инфраструктуры в защищенном исполнении.

Планируемые результаты обучения по модулю:

В результате освоения модуля у слушателей должны быть сформированы следующие **компетенции**:

– способность проектировать сетевую корпоративную информационную инфраструктуру в защищенном исполнении;

– способность применять знания в области технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов информационных систем в сфере профессиональной деятельности;

– системное и критическое мышление в цифровой среде.

В результате освоения модуля обучающийся должен:

Знать:

– общие принципы построения сетей;

– современные стандарты информационного взаимодействия систем;

– классификацию современных программных и программно-аппаратных СЗИ;

– состав, назначение функциональных компонентов и программного обеспечения программных и программно-аппаратных СЗИ;

– типовые структуры и принципы организации программных и программно-аппаратных СЗИ;

– алгоритмы анализа информационного пространства.

Уметь:

– реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования;

– проводить комплексное тестирование и отладку программных систем;

– организовывать сетевую корпоративную информационную инфраструктуру в защищенном исполнении;

– работать с интегрированной средой разработки программного обеспечения;

– эффективно использовать полученную информацию для создания новых программных решений сложных задач в условиях неопределенности;

– осуществлять сбор, обработку, анализ и систематизацию научно- технической информации в области программных и программно-аппаратных СЗИ и систем с применением современных информационных технологий;

– передавать информацию с помощью цифровых средств.

Владеть:

– принципами использования современных языков программирования высокого уровня;

– процедурой организации обработки и хранения персональных данных в соответствии с требованиями законодательства;

– способами использования возможностей компьютера и цифровой среды для решения

профессиональных задач;
- эффективными способами использования полученной информации для решения сложных задач в условиях неопределенности.

Содержание модуля:

№, наименование темы	Содержание лекций (количество часов)	Наименование практических занятий (количество часов)	Виды СРС (количество часов)
1. Разработка ПО	Массивы и строки. Создание форм. Элементы управления форм для работы с массивами. Организация взаимодействия приложения с пользователем Постановка задачи: – изучить понятия: Массивы и строки. Создание форм. Элементы управления форм для работы с массивами. Организация взаимодействия приложения с пользователем. Предполагаемый результат действия: – усвоен материал темы. Предполагаемая форма результата деятельности: – опорный конспект лекций. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с выходом в Интернет. Критерии оценки деятельности: – 1 балл: отмечены опорные точки, применен опорный конспект для своего примера. – 0 балла: опорный конспект отсутствует. Характер деятельности: индивидуальный (10)	Получение навыков разработки ПО в C#; Изучение функционала элементов управления форм; Организация взаимодействия приложения с пользователем Постановка задачи: – получить навыки разработки ПО в C#; – Изучить функционал элементов управления форм; – Организовать взаимодействие приложения с пользователем. Предполагаемый результат действия: – приложения Windows Forms. Предполагаемая форма результата деятельности: – программный код. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с установленной средой разработки и выходом в Интернет. Критерии оценки деятельности: – 3 балла: 3 из 3 заданий выполнены успешно (функционал разработанных консольных приложений реализован в полном объеме); – 2 балла: 2 из 3 заданий выполнены успешно (функционал разработанных приложений реализован в полном объеме); – 1 балл: 1 из 3 заданий выполнены успешно (функционал разработанных приложений реализован в полном объеме); – 0 баллов: 0 из 3 заданий выполнены успешно (функционал разработанных приложений не реализован в полном объеме); Характер деятельности:	Закрепить навыки написания приложений Windows Forms Постановка задачи: – Закрепить навыки написания приложений Windows Forms. Предполагаемый результат действия: – приложение Windows Forms. Предполагаемая форма результата деятельности: – программный код. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с установленной средой разработки и выходом в Интернет. Критерии оценки деятельности: – 1 балл: функционал разработанного приложения Windows Forms реализован в полном объеме; – 0 баллов: функционал разработанного приложения Windows Forms не реализован в полном объеме; Характер деятельности: индивидуальный (25)

		индивидуальный (15)	
2. Сети и системы передачи информации	Сетевая модель OSI. Сетевые устройства. Построение информационной корпоративной инфраструктуры. Атаки на сетевые инфраструктуры. Постановка задачи: – изучить понятия: модель OSI и ее уровни, виды атак на сетевые устройства. Предполагаемый результат действия: – усвоен материал темы. Предполагаемая форма результата деятельности: – опорный конспект лекций. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с выходом в Интернет. Критерии оценки деятельности: – 1 балл: отмечены опорные точки, применен опорный конспект для своего примера. – 0 балла: опорный конспект отсутствует. Характер деятельности: индивидуальный (20)	Навыки проектирования корпоративной инфраструктуры. Постановка задачи: – получить навыки настройки сетевых устройств; Предполагаемый результат действия: – настроить сеть по заданным параметрам в виртуальной лаборатории. Предполагаемая форма результата деятельности: – настроенная виртуальная сеть. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с установленной средой виртуализации и выходом в Интернет. Критерии оценки деятельности: – 2 балла: настройка сети реализована в полном объеме; – 1 балл: настройка сети реализована частично; – 0 баллов: настройка сети не реализован. Характер деятельности: индивидуальный (15)	Закрепить навыки проектирования корпоративной инфраструктуры. Постановка задачи: – Закрепить навыки проектирования корпоративной инфраструктуры; Предполагаемый результат действия: - настроить сеть по заданным параметрам в виртуальной лаборатории. Предполагаемая форма результата деятельности: - настроенная виртуальная сеть. Перечень инструментов, необходимых для реализации деятельности: - персональный компьютер с установленной средой виртуализации и выходом в Интернет. Критерии оценки деятельности: - 2 балла: настройка сети реализована в полном объеме; - 1 балл: настройка сети реализована частично; - 0 баллов: настройка сети не реализован. Характер деятельности: индивидуальный (25)

Оценка качества освоения модуля

2.3.1. Форма промежуточной аттестации – зачет.

Пример заданий к зачету:

Создать Windows-приложение для расчета индекса цифровой грамотности населения (ИЦГН) на основе обработки данных опроса населения (вопросы для опроса необходимо придумать так, чтобы по ним можно было вычислить ИЦГН по 10-ти бальной шкале). ИЦГН рассчитывать как зависимость между 3 показателями: уровень цифровых компетенций, уровень цифрового потребления и уровень цифровой безопасности. Анкету пользователь заполняет с формы приложения. В первом окне пользователь вводит свои данные. Затем появляются вопросы. Вопросы в анкете должны предполагать различные виды ответов: текстовый ответ, выбор, логический выбор, сопоставление.

2.3.2. Оценочные материалы

Оценивание задания:

Критерий оценивания	Количество баллов	Характеристика
Вопросы для теста	0	Вопросы не относятся к теме ИЦГН
	1	Вопросы не охватывают все 3 показателя
	2	Вопросы полностью охватывают все 3 показателя ИЦГН
Стиль оформления программного кода	1	Не структурирован
	2	Структурирован и присутствуют комментарии
Взаимодействие с	0	Пользователю ПО не понятно, что надо делать

пользователем		в приложении и не продуман интерфейс ПО
	1	Графический интерфейс программы проработан не достаточно и пользователю сложно разобраться в нем
	2	Удобный графический интерфейс ПО
Использование графических элементов	0	Не использованы
	2	Использованы
Расчет в процентах ИЦГН	0	Не рассчитан
	1	Рассчитан только общий процент ИЦГН
	2	Рассчитан общий процент ИЦГН и по каждому показателю

шкала оценивания:

Количество набранных баллов	Результат
0-5	не удовлетворительно
6-7	удовлетворительно
7-8	хорошо
9-10	отлично

2.3.3. Методические материалы

Методические рекомендации по работе с порталом дистанционного обучения [Электронный ресурс]: URL: https://clck.ru/SuPoX

Организационно-педагогические условия реализации дисциплины:

а) Материально-технические условия

Вид ресурса	Характеристика ресурса
Аудитория	—
Компьютерный класс	—
Программное обеспечение	– Visual Studio Community или Visual Studio Code или аналогичное ПО для создания приложений на языке программирования C#; – Яндекс.Браузер, Веб-браузер Google Chrome или аналогичное ПО – Microsoft Office или LibreOffice или аналогичное офисное ПО. – Пакет OpenSSL.
Канцелярские товары	—
Условия для функционирования электронной информационно-образовательной среды (при использовании ДОТ)	http://m.idpo.magtu.ru/course/view.php?id=291

б) Учебно-методическое и информационное обеспечение

Вид ресурса	Характеристика ресурса
Нормативные правовые акты/регламенты	1. Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», от 15.09.2016 № 522н
Литература	Учебная литература: – Гуриков, С. Р. Введение в программирование на языке Visual C# : учебное пособие / С.Р. Гуриков. — Москва : ФОРУМ : ИНФРА-М, 2020. — 447 с. – Хорев, П. Б. Объектно-ориентированное программирование с примерами на C# : учебное пособие / П.Б. Хорев. — Москва : ФОРУМ :

	ИНФРА-М, 2020. — 200 с.
Электронные ресурсы	https://metanit.com/ http://window.edu.ru/ https://bdu.fstec.ru/ https://cybermap.kaspersky.com/ru https://www.ptsecurity.com/ru-ru/
Методические материалы	Методические разработки: – Видеолекция «Установка MS VS Com 2019»; – Видеолекция «Работа с массивами»; – Видеолекция «Работа с массивами. Змейка»; – Видеолекция «Работа с текстом»; – Видеолекция «Работа с текстовым файлом»; разработаны и размещены на портале дистанционного обучения http://m.idpo.magtu.ru/ 1. Бабарыкина И.Н., Субботина Е.В. Электронно-образовательный ресурс «Организация самостоятельной работы студентов: Учебно-методическое пособие». - Магнитогорск: ФГБОУ ВПО «МГТУ», 2012. 2. Методические рекомендации по работе с порталом дистанционного обучения [Электронный ресурс]: URL: https://clck.ru/SuPoX
Раздаточные материалы	—

в) Кадровые условия

Кадровое обеспечение осуществляют преподаватели кафедры ИиИБ ФГБОУ ВО «МГТУ им. Г. И. Носова»

Модуль 2. Безопасность сетей ЭВМ

Цель освоения модуля

Целью освоения модуля является формирование профессиональных компетенций специалиста в области организации защиты сетевых устройств и каналов передачи информации, обнаружения и предотвращения несанкционированного доступа к информации в сетях ЭВМ, а так же владение принципам построения систем защиты информации в локальных вычислительных сетях (ЛВС) и методам анализа надежности защиты ЛВС.

Планируемые результаты обучения по модулю:

В результате освоения модуля у слушателей должны быть сформированы следующие **компетенции**:

– способность проектировать сетевую корпоративную информационную инфраструктуру в защищенном исполнении;

– способен применять знания в области безопасности вычислительных сетей при разработке корпоративных информационных систем.

В результате освоения модуля обучающийся должен:

Знать:

– общие принципы построения сетей;
– знать физические принципы передачи информации по различным каналам связи;
– знать и понимать характерные уязвимости, присущие каналами связи при передаче информации по ним;
– четко представлять методы перехвата информации при передаче ее по различным каналам связи.

Уметь:

– самостоятельно диагностировать неисправность или аномалию работы сети ЭВМ;
– сделать самостоятельное заключение о возможности или невозможности

несанкционированного доступа к информации при данной неисправности сети;
- предложить комплекс мер по устранению неисправности и предотвращению несанкционированного доступа к информации сети ЭВМ;
- разработать комплекс мер для контроля безотказного функционирования сетей ЭВМ;

Владеть:

- способностью к самостоятельному анализу тенденций развития технологий современных глобальных и локальных вычислительных сетей с точки зрения специалиста по информационной безопасности;
- способностью прогнозировать потребности организации в технологиях защиты информации в сетях ЭВМ исходя из характера хозяйственной деятельности организации и обрабатываемой ею информации;
- навыками настройки сетевого оборудования (коммутатор, маршрутизатор, межсетевой экран) для построения разработанной топологии сети и соблюдения требований по защите информации.

Содержание модуля:

№, наименование темы	Содержание лекций (количество часов)	Наименование практических занятий (количество часов)	Виды СРС (количество часов)
1. Модель безопасности для локальной вычислительной сети	Сегментирование ЛВС как способ повышения безопасности сети. Принцип «обороны в глубину» как базовый принцип при организации защиты сети. Постановка задачи: – изучить понятия: Принцип «обороны в глубину». Сегментирование ЛВС. Предполагаемый результат действия: – усвоен материал темы. Предполагаемая форма результата деятельности: – опорный конспект лекций. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с выходом в Интернет. Критерии оценки деятельности: – 1 балл: отмечены опорные точки, применен опорный конспект для своего примера. – 0 балла: опорный конспект отсутствует. Характер деятельности: индивидуальный (15)	Получение навыков проектирования сетей в защищенном исполнении. Постановка задачи: – получить навыки проектирования сети в защищенном исполнении; Предполагаемый результат действия: – настроить сеть по заданным параметрам в виртуальной лаборатории. Предполагаемая форма результата деятельности: – настроенная виртуальная сеть. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с установленной средой виртуализации и выходом в Интернет. Критерии оценки деятельности: – 2 балла: настройка сети реализована в полном объеме; – 1 балл: настройка сети реализована частично; – 0 баллов: настройка сети не реализован. Характер деятельности: индивидуальный (20)	Закрепить навыки проектирования сетей в защищенном исполнении. Постановка задачи: Закрепить навыки проектирования корпоративной инфраструктуры; Предполагаемый результат действия: - настроить сеть по заданным параметрам в виртуальной лаборатории. Предполагаемая форма результата деятельности: - настроенная виртуальная сеть. Перечень инструментов, необходимых для реализации деятельности: - персональный компьютер с установленной средой виртуализации и выходом в Интернет. Критерии оценки деятельности: - 2 балла: настройка сети реализована в полном объеме; - 1 балл: настройка сети реализована частично; - 0 баллов: настройка сети не реализован. Характер деятельности: индивидуальный (30)
2. Обнаружение и нейтрализация сетевых атак	Фазы сетевой атаки. Методики обнаружения сетевых атак. Технология	Навыки проектирования корпоративной инфраструктуры с применением	Закрепить навыки проектирования корпоративной инфраструктуры с применением

	виртуальных ЛВС (VLAN). Технология списков контроля доступа (ACL). Технология Port Security. Постановка задачи: – изучить технологии: Port Security, ACL, VLAN. Предполагаемый результат действия: – усвоен материал темы. Предполагаемая форма результата деятельности: – опорный конспект лекций. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с выходом в Интернет. Критерии оценки деятельности: – 1 балл: отмечены опорные точки, применен опорный конспект для своего примера. – 0 балла: опорный конспект отсутствует. Характер деятельности: индивидуальный (15)	изученных технологий. Постановка задачи: – получить навыки настройки сети с применением изученных технологий; Предполагаемый результат действия: – настроить сеть по заданным параметрам в виртуальной лаборатории. Предполагаемая форма результата деятельности: – настроенная виртуальная сеть. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с установленной средой виртуализации и выходом в Интернет. Критерии оценки деятельности: – 2 балла: настройка сети реализована в полном объеме; – 1 балл: настройка сети реализована частично; – 0 баллов: настройка сети не реализован. Характер деятельности: индивидуальный (20)	изученных технологий. Постановка задачи: – Закрепить навыки настройки сети с применением изученных технологий; Предполагаемый результат действия: - настроить сеть по заданным параметрам в виртуальной лаборатории. Предполагаемая форма результата деятельности: - настроенная виртуальная сеть. Перечень инструментов, необходимых для реализации деятельности: - персональный компьютер с установленной средой виртуализации и выходом в Интернет. Критерии оценки деятельности: - 2 балла: настройка сети реализована в полном объеме; - 1 балл: настройка сети реализована частично; - 0 баллов: настройка сети не реализован. Характер деятельности: индивидуальный (40)

Оценка качества освоения модуля

2.3.1. Форма промежуточной аттестации – экзамен.

Пример заданий к экзамену:

Настроить сеть по заданию и произвести фильтрацию трафика вычислительной сети с помощью свободно распространяемых программ-анализаторов WireShark или Ethereal.

2.3.2. Оценочные материалы

Оценивание задания:

Критерий оценивания	Количество баллов	Характеристика
Сеть настроена по указанным параметрам	0	Пользователю ПО не понятно, что надо делать и не выполнена настройка сети
	5	Сеть настроена, но не полностью заданы параметры
	7	Сеть настроена в соответствии с заданием
Фильтрация трафика	0	Не выполнена
	5	Выполнена

шкала оценивания:

Количество набранных баллов	Результат
0-4	не удовлетворительно
5-7	удовлетворительно
7-9	хорошо
10-12	отлично

2.3.3. Методические материалы

Методические рекомендации по работе с порталом дистанционного обучения [Электронный ресурс]: URL: https://clck.ru/SuPoX

Организационно-педагогические условия реализации дисциплины:
а) Материально-технические условия

Вид ресурса	Характеристика ресурса
Аудитория	Лаборатория сетей и систем передачи данных с комплектом типового учебного оборудования "Сетевая безопасность типа SECURITY-3M"
Компьютерный класс	—
Программное обеспечение	– Яндекс.Браузер, Веб-браузер Google Chrome или аналогичное ПО –
Канцелярские товары	—
Условия для функционирования электронной информационно-образовательной среды (при использовании ДОТ)	http://m.idpo.magtu.ru/course/view.php?id=291

б) Учебно-методическое и информационное обеспечение

Вид ресурса	Характеристика ресурса
Нормативные правовые акты/регламенты	1. Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», от 15.09.2016 № 522н
Литература	Учебная литература: – Сети и телекоммуникации : учебник и практикум для вузов / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2020. — 363 с. — (Высшее образование). — ISBN 978-5-534-00949-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450234 (дата обращения: 12.03.2020). – Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1: учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 333 с. — (Высшее образование). — ISBN 978-5-9916-9956-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452430 (дата обращения: 12.03.2020). – Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2: учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 351 с. — (Высшее образование). — ISBN 978-5-9916-9958-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/453063 (дата обращения: 12.03.2020)..
Электронные ресурсы	https://bdu.fstec.ru/ https://cybermap.kaspersky.com/ru https://www.ptsecurity.com/ru-ru/
Методические материалы	- Сетевая защита информации. Лабораторный практикум : учебное пособие [для вузов] / Д. Н. Мазнин [и др.] ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3824.pdf&show=dcatalogues/1/1530260/3824.pdf&view=true (дата обращения: 22.10.2019). -

	Макрообъект. - ISBN 978-5-9967-1605-0. - Текст: электронный. - Сведения доступны также на CD-ROM.
Раздаточные материалы	—

в) Кадровые условия

Кадровое обеспечение осуществляют преподаватели кафедры ИиИБ ФГБОУ ВО «МГТУ им. Г. И. Носова»

Модуль 3. Организационно-правовые основы технической защиты конфиденциальной информации

Цель освоения модуля

Целью освоения модуля является формирование профессиональных компетенций специалиста в области основ кибербезопасности и организационной защиты информации, в области изучения источников и классификации угроз информационной безопасности.

Планируемые результаты обучения по модулю:

В результате освоения модуля у слушателей должны быть сформированы следующие **компетенции**:

– способность оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

– способность оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями.

– способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объектов защиты.

В результате освоения модуля обучающийся должен:

Знать:

– основы цифровой гигиены;

– отличия законодательства РФ и других стран в сфере кибербезопасности;

– способы оформления документации по регламентации мероприятий и оказанию услуг в области защиты информации;

– типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях;

– характерные уязвимости, присущие каналами связи сетей ЭВМ при передаче информации по ним;

– организационные меры по защите информации;

– основные методики противодействия перехвату и несанкционированному съему информации при ее передаче по каналам связи сетей ЭВМ;

– классификацию и основные принципы действия оборудования и ПО, предназначенного для организации защищенных каналов передачи информации;

– особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах.

Уметь:

– анализировать статистику реализации различных видов угроз;

– оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;

– осуществлять поиск новой методической документации по регламентации мероприятий и оказанию услуг в области защиты информации;

– пользоваться банком угроз ФСТЭК России;

– разрабатывать проекты нормативных и организационно- распорядительных

документов, регламентирующих работу по защите информации;
- применять действующую нормативную базу при обеспечении безопасности сетей ЭВМ;
- определять основные угрозы безопасности в сетях ЭВМ.

Владеть:
- способами анализа степени опасности угроз;
- методиками определения и поиска уязвимостей систем защиты информации в сетях ЭВМ;
- приемами определения и классификации сетевых атак;
- методологией составления политик сетевой безопасности;
- навыками работы с нормативными правовыми актами, нормотворческой деятельности, работы с законами и иными нормативными правовыми актами и применения их на практике.

Содержание модуля:

№, наименование темы	Содержание лекций (количество часов)	Наименование практических занятий (количество часов)	Виды СРС (количество часов)
1. Кибербезопасность как один из ключевых факторов устойчивого развития цифровой экономики. Законодательство РФ в области информационной безопасности. Ответственность.	Освоение понятий «Кибербезопасность, защита информации». Изучить законодательство в сфере ИБ Постановка задачи: – изучить понятия: кибербезопасность, защита информации. Изучить законодательство в сфере ИБ. Предполагаемый результат действия: – усвоен материал по темам: «Кибербезопасность как один из ключевых факторов устойчивого развития цифровой экономики». Предполагаемая форма результата деятельности: – опорный конспект лекций. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с выходом в Интернет. Критерии оценки деятельности: – 1 балл: отмечены опорные точки, применен опорный конспект для своего примера. – 0 балла: опорный конспект отсутствует. Характер деятельности: индивидуальный (5)	Навыки работы с интерактивной картой угроз на сайте Касперского Постановка задачи: – получить навыки работы с интерактивной картой угроз на сайте Касперского; Предполагаемый результат действия: – сбор статистики. Предполагаемая форма результата деятельности: – отчет. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с установленной средой разработки и выходом в Интернет. Критерии оценки деятельности: – 3 балла: статистика собрана в полном объеме более чем с одного ресурса; – 2 балла: статистика собрана в полном объеме; – 1 балл: статистика собрана частично – 0 баллов: статистика не собрана. Характер деятельности: индивидуальный (5)	Навыки работы с другими ресурсами по ИБ Постановка задачи: – Закрепить навыки работы с другими ресурсами по ИБ. Предполагаемый результат действия: – сбор статистики. Предполагаемая форма результата деятельности: – отчет. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с установленной средой разработки и выходом в Интернет. Критерии оценки деятельности: – 2 балла: статистика собрана в полном объеме. – 1 балл: статистика собрана частично; – 0 баллов: статистика не собрана; Характер деятельности: индивидуальный (20)
2. Понятие организационной защиты информации. Источники и классификация угроз	Организационная защита информации, угрозы ИБ, персональные данные. Изучить	Разработка схемы деятельности должностных лиц для обеспечения информационной	Провести сравнительный анализ видов тайн Постановка задачи: – Провести сравнительный анализ видов тайн.

информационной безопасности. Защита персональных данных	законодательство в сфере защиты ПДн Постановка задачи: – изучить понятия: организационная защита информации, угрозы ИБ, персональные данные. Изучить законодательство в сфере защиты ПДн. Предполагаемый результат действия: – усвоен материал по темам: «Понятие организационной защиты информации. Источники и классификация угроз информационной безопасности. Защита персональных данных». Предполагаемая форма результата деятельности: – опорный конспект лекций. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с выходом в Интернет. Критерии оценки деятельности: – 1 балл: отмечены опорные точки, применен опорный конспект для своего примера. – 0 балла: опорный конспект отсутствует. Характер деятельности: индивидуальный (5)	безопасности Постановка задачи: – получить навыки разработки схемы деятельности должностных лиц для обеспечения информационной безопасности; Предполагаемый результат действия: – разработанная схема деятельности. Предполагаемая форма результата деятельности: – Mind карта. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с установленной средой разработки и выходом в Интернет. Критерии оценки деятельности: – 3 балла: Mind карта реализована в полном объеме с учетом особенностей выбранной организации; – 2 балла: Mind карта выполнена в полном объеме, но для типового примера; – 1 балл: Mind карта собрана частично – 0 баллов: Mind карта не собрана. Характер деятельности: индивидуальный (10)	Предполагаемый результат действия: – сбор статистики и анализ. Предполагаемая форма результата деятельности: – сводная таблица. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с установленной средой разработки и выходом в Интернет. Критерии оценки деятельности: – 2 балла: статистика собрана в полном объеме и проведен анализ. – 1 балл: статистика собрана частично, анализ не закончен до конца; – 0 баллов: статистика не собрана, анализ не проведен; Характер деятельности: индивидуальный (40)
3. Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. Основные принципы создания системы управления информационной безопасностью. Разработка политик информационной безопасности.	СЗИ, политика ИБ, СУИБ Постановка задачи: – изучить понятия: СЗИ, политика ИБ, СУИБ. Предполагаемый результат действия: – усвоен материал по темам: «Основные средства и способы обеспечения информационной безопасности. Системы защиты информации. Управление ИБ». Предполагаемая форма результата деятельности: – опорный конспект лекций. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с выходом в Интернет. Критерии оценки деятельности: – 1 балл: отмечены опорные точки, применен опорный конспект для своего примера. – 0 балла: опорный конспект отсутствует. Характер деятельности: индивидуальный (10)	Получение навыков разработки парольной политики для своей организации Постановка задачи: – получить навыки разработки парольной политики для своей организации; Предполагаемый результат действия: – разработанная политика. Предполагаемая форма результата деятельности: – оформленная политика в виде файла. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с установленной средой разработки и выходом в Интернет. Критерии оценки деятельности: – 3 балла: политика реализована в полном объеме с учетом особенностей выбранной организации; – 2 балла: политика выполнена в полном объеме, но для типового примера;	Сравнительный анализ средств антивирусной защиты для ПК и смартфона Постановка задачи: – Провести сравнительный анализ средств антивирусной защиты для ПК и смартфона. Предполагаемый результат действия: – сбор статистики и анализ. Предполагаемая форма результата деятельности: – сводная таблица. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с установленной средой разработки и выходом в Интернет. Критерии оценки деятельности: – 2 балла: статистика собрана в полном объеме и проведен анализ. – 1 балл: статистика

		– 1 балл: политика собрана частично – 0 баллов: политика не собрана. Характер деятельности: индивидуальный (15)	собрана частично, анализ не закончен до конца; – 0 баллов: статистика не собрана, анализ не проведен; Характер деятельности: индивидуальный (40)

Оценка качества освоения модуля

2.3.1. Форма промежуточной аттестации – экзамен.

Пример заданий к экзамену:

Постройте дерево атак с учетом вероятности возникновения угроз на основе статистики за 2022 год по данным «Лаборатории Касперского». Ответ предоставить в виде файла с построенным деревом атак.

2.3.2. Оценочные материалы

Оценивание задания:

Критерий оценивания	Количество баллов	Характеристика
Программное обеспечение, в котором выполнен проект	0	Скриншот рисунка на бумаге
	1	Microsoft Word (или другие схожие по функционалу программы)
	2	Microsoft Visio (или другие схожие по функционалу программы)
Стиль оформления дерева атак	0	Описан в виде не систематизированного текста
	2	Оформлен в виде концептуальной диаграммы (дерева)
Выбор угроз	0	Выбраны не актуальные угрозы
	1	Выбраны частично актуальные угрозы
	2	Выбраны актуальные угрозы
Использование данных «Лаборатории Касперского» за 2022 год	0	Не использованы
	2	Использованы

шкала оценивания:

Количество набранных баллов	Результат
0-3	не удовлетворительно
4-5	удовлетворительно
6-7	хорошо
8	отлично

2.3.3. Методические материалы

Методические рекомендации по работе с порталом дистанционного обучения [Электронный ресурс]: URL: https://clck.ru/SuPoX

Организационно-педагогические условия реализации дисциплины:

а) Материально-технические условия

Вид ресурса	Характеристика ресурса
Аудитория	-
Компьютерный класс	-
Программное обеспечение	– Яндекс.Браузер, Веб-браузер Google Chrome или аналогичное ПО – Microsoft Office или LibreOffice или аналогичное офисное ПО.

	– Пакет OpenSSL.
Канцелярские товары	-
Условия для функционирования электронной информационно-образовательной среды (при использовании ДОТ)	http://m.idpo.magtu.ru/course/view.php?id=291

б) Учебно-методическое и информационное обеспечение

Вид ресурса	Характеристика ресурса
Нормативные правовые акты/регламенты	1. Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», от 15.09.2016 № 522н
Литература	Методические разработки: – Видеолекция. Технические средства обеспечения защиты информации; разработаны и размещены на портале дистанционного обучения http://m.idpo.magtu.ru/ Учебная литература: - Ищукова, Е. А. Криптографические протоколы и стандарты: Учебное пособие / Ищукова Е.А., Лобова Е.А. - Таганрог:Южный федеральный университет, 2016. - 80 с.: ISBN 978-5-9275-2066-4. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/991903 - Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772(дата обращения: 24.02.2020). - Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин
Электронные ресурсы	https://metanit.com/ http://window.edu.ru/ https://bdu.fstec.ru/ https://cybermap.kaspersky.com/ru https://www.ptsecurity.com/ru-ru/
Методические материалы	1. Бабарыкина И.Н., Субботина Е.В. Электронно-образовательный ресурс «Организация самостоятельной работы студентов: Учебно-методическое пособие». - Магнитогорск: ФГБОУ ВПО «МГТУ», 2012. 2. Методические рекомендации по работе с порталом дистанционного обучения [Электронный ресурс]: URL: https://clck.ru/SuPoX
Раздаточные материалы	—

в) Кадровые условия

Кадровое обеспечение осуществляют преподаватели кафедры ИиИБ ФГБОУ ВО «МГТУ им. Г. И. Носова»

Модуль 4. Организация защиты конфиденциальной информации на ОИ

Целью освоения модуля является формирование профессиональных компетенций специалиста в области организационной защиты конфиденциальной информации.

Планируемые результаты обучения по модулю:

В результате освоения модуля у слушателей должны быть сформированы следующие **компетенции**:

– способность оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

– способность оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями.

– способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объектов защиты.

В результате освоения модуля обучающийся должен:

Знать:

– способы оформления документации по регламентации мероприятий и оказанию услуг в области защиты конфиденциальной информации;

– типовые средства и методы защиты конфиденциальной информации в локальных и глобальных вычислительных сетях;

– характерные уязвимости, присущие каналами связи сетей ЭВМ при передаче конфиденциальной информации по ним;

– организационные меры по защите конфиденциальной информации.

Уметь:

– оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты конфиденциальной информации;

– осуществлять поиск новой методической документации по регламентации мероприятий и оказанию услуг в области защиты конфиденциальной информации;

– разрабатывать проекты нормативных и организационно- распорядительных документов, регламентирующих работу по защите конфиденциальной информации.

Владеть:

– способами анализа степени опасности угроз конфиденциальной информации;

– методологией составления политик информационной безопасности конфиденциальной информации;

– навыками работы с нормативными правовыми актами, нормотворческой деятельности, работы с законами и иными нормативными правовыми актами и применения их на практике для защиты конфиденциальной информации.

Содержание модуля:

№, наименование темы	Содержание лекций (количество часов)	Наименование практических занятий (количество часов)	Виды СРС (количество часов)
1. Законодательство РФ в области информационной безопасности конфиденциальной информации. Ответственность.	Освоение понятия «Конфиденциальная информация». Изучить законодательство в сфере ИБ конфиденциальной	Навыки работы с нормативно-методической документацией в области защиты конфиденциальной информации.	Навыки работы с нормативно-методической документацией в области защиты конфиденциальной информации.

	информации. Постановка задачи: – изучить понятия: конфиденциальная информация. Изучить законодательство в этой сфере. Предполагаемый результат действия: – усвоен материал по теме. Предполагаемая форма результата деятельности: – опорный конспект лекций. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с выходом в Интернет. Критерии оценки деятельности: – 1 балл: отмечены опорные точки, применен опорный конспект для своего примера. – 0 балла: опорный конспект отсутствует. Характер деятельности: индивидуальный (5)	Постановка задачи: – получить навыки работы с нормативно-методической документацией в области защиты конфиденциальной информации; Предполагаемый результат действия: – сбор и анализ статистики нормативной базы. Предполагаемая форма результата деятельности: – отчет. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с установленной средой разработки и выходом в Интернет. Критерии оценки деятельности: – 3 балла: статистика собрана в полном объеме более чем с одного ресурса; – 2 балла: статистика собрана в полном объеме; – 1 балл: статистика собрана частично – 0 баллов: статистика не собрана. Характер деятельности: индивидуальный (15)	Постановка задачи: – получить навыки работы с нормативно-методической документацией в области защиты конфиденциальной информации; Предполагаемый результат действия: – сбор и анализ статистики нормативной базы. Предполагаемая форма результата деятельности: – отчет. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с установленной средой разработки и выходом в Интернет. Критерии оценки деятельности: – 2 балла: статистика собрана в полном объеме. – 1 балл: статистика собрана частично; – 0 баллов: статистика не собрана; Характер деятельности: индивидуальный (20)
2. Основные средства и способы обеспечения информационной безопасности конфиденциальной информации. Разработка политик информационной безопасности конфиденциальной информации.	СЗИ, политика ИБ. Постановка задачи: – изучить понятия: СЗИ, политика ИБ. Предполагаемый результат действия: – усвоен материал по теме. Предполагаемая форма результата деятельности: – опорный конспект лекций. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с выходом в Интернет. Критерии оценки деятельности: – 1 балл: отмечены опорные точки, применен опорный конспект для своего примера. – 0 балла: опорный конспект отсутствует. Характер деятельности: индивидуальный (5)	Получение навыков разработки политики для организации защиты конфиденциальной информации. Постановка задачи: – получить навыки разработки политики; Предполагаемый результат действия: – разработанная политика. Предполагаемая форма результата деятельности: – оформленная политика в виде файла. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с установленной средой разработки и выходом в Интернет. Критерии оценки деятельности: – 3 балла: политика реализована в полном объеме с учетом особенностей выбранной организации; – 2 балла: политика выполнена в полном объеме, но для типового примера; – 1 балл: политика собрана частично – 0 баллов: политика не	Сравнительный анализ политик на примере реальных организаций Постановка задачи: – Провести сравнительный анализ политик ИБ. Предполагаемый результат действия: – сбор информации и анализ. Предполагаемая форма результата деятельности: – сводная таблица. Перечень инструментов, необходимых для реализации деятельности: – персональный компьютер с установленной средой разработки и выходом в Интернет. Критерии оценки деятельности: – 2 балла: статистика собрана в полном объеме и проведен анализ. – 1 балл: статистика собрана частично, анализ не закончен до конца; – 0 баллов: статистика не собрана, анализ не проведен; Характер деятельности: индивидуальный (20)

		собрана. Характер деятельности: индивидуальный (25)	

Оценка качества освоения модуля

2.3.1. Форма промежуточной аттестации – зачет.

Пример вопросов к зачету:

Назовите перечень сведений конфиденциального характера согласно нормативной базе РФ.

2.3.2. Оценочные материалы

Оценивание вопроса:

Критерий оценивания	Количество баллов	Характеристика
Полнота перечня	0	Не названо ни одного пункта
	1	Перечень назван частично
	2	Перечень назван полностью
Разъяснения пунктов перечня	0	Перечислены только понятия без указания нормативных актов, в которых это описывается
	1	Дано частичное пояснения пунктов перечня
	2	Дано полное пояснения всех пунктов перечня

шкала оценивания:

Количество набранных баллов	Результат
0-2	не зачтено
3-4	зачтено

2.3.3. Методические материалы

Методические рекомендации по работе с порталом дистанционного обучения [Электронный ресурс]: URL: https://clck.ru/SuPoX

Организационно-педагогические условия реализации дисциплины:

а) Материально-технические условия

Вид ресурса	Характеристика ресурса
Аудитория	-
Компьютерный класс	-
Программное обеспечение	– Яндекс.Браузер, Веб-браузер Google Chrome или аналогичное ПО – Microsoft Office или LibreOffice или аналогичное офисное ПО. – Пакет OpenSSL.
Канцелярские товары	-
Условия для функционирования электронной информационно-образовательной среды (при использовании ДОТ)	http://m.idpo.magtu.ru/course/view.php?id=291

б) Учебно-методическое и информационное обеспечение

Вид ресурса	Характеристика ресурса
Нормативные правовые акты/регламенты	1. Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», от 15.09.2016 № 522н
Литература	Методические разработки: – Видеолекция. Технические средства

	обеспечения защиты информации; разработаны и размещены на портале дистанционного обучения http://m.idpo.magtu.ru/ Учебная литература: - Ищукова, Е. А. Криптографические протоколы и стандарты: Учебное пособие / Ищукова Е.А., Лобова Е.А. - Таганрог:Южный федеральный университет, 2016. - 80 с.: ISBN 978-5-9275-2066-4. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/991903 - Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772(дата обращения: 24.02.2020). - Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин
Электронные ресурсы	https://metanit.com/ http://window.edu.ru/ https://bdu.fstec.ru/ https://cybermap.kaspersky.com/ru https://www.ptsecurity.com/ru-ru/
Методические материалы	1. Бабарыкина И.Н., Субботина Е.В. Электронно-образовательный ресурс «Организация самостоятельной работы студентов: Учебно-методическое пособие». - Магнитогорск: ФГБОУ ВПО «МГТУ», 2012. 2. Методические рекомендации по работе с порталом дистанционного обучения [Электронный ресурс]: URL: https://clck.ru/SuPoX
Раздаточные материалы	—

в) Кадровые условия
Кадровое обеспечение осуществляют преподаватели кафедры ИиИБ ФГБОУ ВО «МГТУ им. Г. И. Носова»

3 ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

3.1. Входная диагностика
Длительность входного контроля – 1 час.
Количество вопросов – 36.
Оценивание входного контроля производится следующим образом: вопросы разного уровня сложности, включая вопросы с кейс-заданиями. Баллы за вопрос выставляются в зависимости от сложности вопросов. В тесте 3 категории сложности вопросов: 28 вопросов-1 балл, 7 вопросов - 5 баллов, 1 вопрос- 10 баллов.
Входное тестирование является обязательным минимумом для пропуска на курс!
Шкала оценивания:

Оценка	Результат
0-58,4	Слушатель не подходит для изучения данной программы.

>58,4	Слушатель готов к прохождению курса.

Категории тем для входного тестирования:

1. Блокчейн и криптовалюта

Пример вопроса: Сопоставьте понятия и их определения. Понятия: Блокчейн; Криптовалюта. Определения: Выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию; Разновидность цифровой валюты, учёт внутренних расчётных единиц которой обеспечивает децентрализованная платёжная система (нет внутреннего или внешнего администратора или какого-либо его аналога), работающая в полностью автоматическом режиме.

2. Облачные и туманные вычисления

Пример вопроса: Верно ли утверждение: IAAS – это инфраструктура для облачных вычислений IBM? Ответы: Да; Нет.

3. Защита персональных данных

Пример вопроса: Какой федеральный закон регулирует отношения, связанные с обработкой персональных данных. В качестве ответа введите номер закона числом.

4. Сети и системы передачи информации

Пример вопроса: IP-адрес 74.123.232.7, Маска сети 255.255.255.0. Рассчитайте Адрес сети и напишите его в качестве ответа.

5. Информационные системы и системы обработки данных

Пример вопроса: В прилагаемом файле выполнить расчеты по заданию.

6. Основы программирования

Пример вопроса: Опишите на языке программирования алгоритм подсчета максимального количества подряд идущих элементов, каждый из которых больше предыдущего, в целочисленном массиве длины 30. Файл с массивом прилагается в текстовом файле. Ответ, полученный в программе, ввести в ответ на вопрос.

3.2. Форма итоговой аттестации – междисциплинарный экзамен в форме выполнения итогового практического задания.

Оценка качества освоения программы осуществляется аттестационной комиссией в форме междисциплинарного экзамена на основе пятибалльной системы оценок по основным разделам программы.

Слушатель считается аттестованным, если имеет положительные оценки (3,4 или 5) по всем разделам программы, выносимым на экзамен.

Пример итогового практического задания:

Создать приложение «Журнал регистрации ПО для обеспечения защиты информации предприятия».

В базе данных, которая подключается к приложению, должна храниться информация:

1. Перечень всего закупленного ПО с полным описанием (ПО заводить в БД реально существующее с описанием требуемых характеристик).

2. Перечень сотрудников имеющих доступ ко всей информации в БД (администраторы БД).

3. Перечень заявок от отделов на закуп нового ПО.

4. Структура предприятия с перечнем АРМ сотрудников с описанием технических характеристик.

5. Перечень установки ПО на АРМы сотрудников.

Оформить вывод отчетной документации:

1) Оформить форму на закупку продления лицензий на имеющееся ПО с учетом срока лицензии и списание ПО с учетом срока действия сертификата, указанного изготовителем. Проверка актуальности ПО должна быть ежедневной с выводом перечня ПО для списания или для поверки продления лицензии (за 4 месяца до окончания срока от текущей даты).

2) Оформить перечень ПО требующего заказа или продления лицензии с учетом поданных заявок (за 4 месяца до окончания срока от текущей даты).

3) Рассчитать расходы предприятия на закупку нового ПО и расходы на продление лицензий.

3.2. Оценочные материалы

Критерий оценивания	Количество баллов	Характеристика
Входная информация храниться в БД	1	Получение входных данных не из БД, а с формы
	2	Получение входных данных из подключенной БД
Стиль оформления программного кода	1	Не структурирован
	2	Структурирован и присутствуют комментарии
Взаимодействие с пользователем	0	Пользователю ПО не понятно, что надо делать в приложении и не продуман интерфейс ПО
	1	Графический интерфейс программы проработан не достаточно и пользователю сложно разобраться в нем
	2	Удобный графический интерфейс ПО
Использование графических элементов	0	Не использованы
	2	Использованы
Выполнен 1 отчет	0	Не выполнен
	1	Рассчитан частично
	2	Рассчитан в полном объеме
Выполнен 2 отчет	0	Не выполнен
	1	Рассчитан частично
	2	Рассчитан в полном объеме
Выполнен 3 отчет	0	Не выполнен
	1	Рассчитан частично
	2	Рассчитан в полном объеме
Для описания ПО в БД использованы данные реального ПО для защиты информации	0	Не использованы
	2	Использованы

шкала оценивания:

Количество набранных баллов	Результат
0-8	не удовлетворительно
9-12	удовлетворительно
13-15	хорошо
15-16	отлично

3.3. Методические материалы

Методические рекомендации по работе с порталом дистанционного обучения [Электронный ресурс]: URL: https://clck.ru/SuPoX

4 СОСТАВИТЕЛИ ПРОГРАММЫ

Перечень составителей программы:

1. У.В. Кузьмина, доцент каф. ИиИБ, кандидат технических наук, доцент по системам и методам защиты информации ФГБОУ ВО «МГТУ им. Г.И. Носова».