МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДЕНА
Ученым советом ФГБОУ ВО «РГЭУ (РИНХ)»
(протокол № 2 от 29.09.2020)
Председатель ученого совета – ректор
_____ Е.Н. Макаренко

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА -
ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Основы личной и корпоративной кибербезопасности в цифровой экономике»

72 час.

Ростов-на-Дону
2020

ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1. Цель программы

Обновление и приобретение глубоких теоретических знаний, формирование и актуализация навыков и общепрофессиональных компетенций в области кибербезопасности и защиты данных. Формирование знания теоретических основ и умения воплотить полученные знания в конкретные формы и механизмы.

2. Планируемые результаты обучения:

Слушатель должен приобрести следующие знания, умения и навыки, необходимые для качественного изменения компетенций:

2.1. Знания

2.1.1. актуальная законодательная и нормативная правовая база, обеспечивающие реализацию мер по защите информации;

2.1.2. основные виды угроз безопасности информации в информационных системах;

2.1.3. содержание и порядок организации работ по выявлению угроз безопасности информации в информационных системах;

2.1.4. знания о методах и средствах обеспечения кибербезопасности.

2.2 Умения:

2.2.1. планировать мероприятия по обеспечению кибербезопасности;

2.2.2. выявлять потенциальные риски и оценивать угрозы безопасности информации в цифровых средах;

2.2.3. определять требования к защищённости информационных систем, в т.ч. информационных систем персональных данных в зависимости от характера угроз;

2.2.4. подбирать и применять методы и средства защиты информации, наиболее релевантные требованиям к защищенности.

2.3 Навыки:

2.3.1. реализации положений законодательной базы и нормативных правовых актов в области обеспечения кибербезопасности;

2.3.2. обеспечения антивирусной защиты устройств, в т.ч. портативных, выявления и нейтрализации вредоносных программ;

2.3.3. выявления угроз и обеспечение безопасности данных, передаваемых по сети Интернет, в т.ч. по беспроводным каналам;

2.3.4. выявления криминально-психологических методов воздействия на пользователя информационных систем и обеспечение устойчивости к кибератакам методами социальной инженерии.

3. Категория слушателей

2.1. Образование: высшее.

2.2. Квалификация: ограничения не устанавливаются.

2.3. Наличие опыта профессиональной деятельности: не требуется.

2.4. Предварительное освоение иных дисциплин: рекомендовано наличие базового уровня знаний по дисциплине «Информационные технологии» или эквивалент(ной/ым) ей.

4. Учебный план программы «Основы личной и корпоративной кибербезопасности в цифровой экономике»

№ п/п	Модуль	Всего, час	Виды учебных занятий		
			Лекции	Практические занятия	Самостоятельная работа
1	Входной контроль	2	-	-	2 (Тест)
2	Модуль 1. Кибербезопасность в условиях цифровой экономики	35	10	-	25
3	Модуль 2. Защита от угроз и конфиденциальность	33	12	-	21
4	Итоговая аттестация	2	-	-	2 (Тест)

5. Календарный план-график реализации образовательной программы

№ п/п	Наименование учебных модулей	Трудоёмкость (час)	Сроки обучения
1	Входной контроль	2	2 ноября
2	Модуль 1. Кибербезопасность в условиях цифровой экономики	35	2-9 ноября 2020 г.
3	Модуль 2. Защита от угроз и конфиденциальность	33	10-16 ноября 2020 г.
4	Итоговая аттестация	2	16 ноября 2020 г.
Всего:		**72**	**15 дней**

6. Учебно-тематический план программы «Основы личной и корпоративной кибербезопасности в цифровой экономике»

№ п/п	Модуль / Тема	Всего, час	Виды учебных занятий			Форма контроля
			Лекции	Практические занятия	Самостоятельная работа	
	Входной контроль	**2**	**-**	**-**	**2**	**Тестирование**
1	**Модуль 1. Кибербезопасность в условиях цифровой экономики**	**35**	**10**	-	**25**	
1.1	Информационная безопасность личности, общества и государства	8	2	-	6	
1.2	Основные понятия и принципы обеспечения кибербезопасности	5	2	-	3	
1.3	Классификация угроз	6	2	-	4	
1.4	Методы и средства обеспечения кибербезопасности в условиях цифровой экономики	8	2	-	6	
1.5	Кибербезопасность в информационной инфраструктуре организации	8	2	-	6	
2	**Модуль 2. Защита от угроз и конфиденциальность**	**33**	**12**	**-**	**21**	
2.1	Вредоносное программное обеспечение и способы защиты от него	7	2	-	5	
2.2	Защита от удаленных сетевых атак	7	2	-	5	
2.3	Защита от атак методами социальной инженерии	7	2	-	5	
2.4	Защита персональных данных в цифровой среде	12	6	-	6	
	Итоговая аттестация	**2**	-	-	**2**	**Тестирование**
	Всего	**72**	**22**	**-**	**50**	

7. Учебная (рабочая) программа повышения квалификации «Основы личной и корпоративной кибербезопасности в цифровой экономике»

Модуль 1. Кибербезопасность в условиях цифровой экономики (35 час.)

Тема 1.1 Информационная безопасность личности, общества и государства (8 час.)

Содержание темы: Информационная безопасность личности, общества и государства в условиях цифровой экономики. Культура кибербезопасности. Морально-этические аспекты кибербезопасности и приватности в информационном пространстве.

Самостоятельная работа по теме 1.1 (6 час.): Роль кибербезопасности в обеспечении национальной безопасности государства. Национальные интересы РФ в информационной сфере. Законодательство в области защиты информации.

Тема 1.2 Основные понятия и принципы обеспечения кибербезопасности (5 час.)

Содержание темы: Понятийный аппарат в области информационной безопасности и кибербезопасности. Целостность, доступность и конфиденциальность. Персональные данные.

Самостоятельная работа по теме 1.2 (3 час.): Принцип экономической эффективности. Принцип усиления слабого звена. Принцип эшелонированности обороны.

Тема 1.3 Классификация угроз (6 час.)
Содержание темы: Источники и виды угроз. Модель угроз информационного ресурса. Модель нарушителя.
Самостоятельная работа по теме 1.3 (4 час.): Модели классификации угроз. Практическое задание «Анализ угроз»
Тема 1.4 Методы и средства обеспечения кибербезопасности в условиях цифровой экономики (8 час.)
Содержание темы: Правовые методы. Организационные методы. Программно-технические методы. Средства идентификации и аутентификации. Управление доступом. Антивирусное программное обеспечение. Межсетевые экраны. Средства резервирования. Шифрование. Электронная подпись.
Самостоятельная работа по теме 1.4 (6 час.): Практическое задание «Выявление требований к защищенности ИС»
Тема 1.5 Кибербезопасность в информационной инфраструктуре организации (8 час.)
Содержание темы: Нормативные требования и стандарты. Особенности реализации угроз на различных уровнях информационной инфраструктуры организации. Последствия реализации угроз.
Самостоятельная работа по теме 1.5 (6 час.): Практическое задание «Подбор СЗИ».

Модуль 2. Защита от угроз и конфиденциальность (33 час.)
Тема 2.1 Вредоносное программное обеспечение и способы защиты от него (7 час.)
Содержание темы: Компьютерная вирусология. Классификация вредоносного ПО. Последствия вирусных атак. Особенности механизмов воздействия вредоносного ПО. Выявление вредоносного ПО. Антивирусные технологии и их практическое применение.
Самостоятельная работа по теме 2.1 (5 час.): Практическое задание «Конфигурирование антивирусного ПО»
Тема 2.2 Защита от удаленных сетевых атак (7 час.)
Содержание темы: Классификация. Последствия атак. Способы обнаружения. Способы защиты. Технология VPN. Безопасность использования беспроводных сетей.
Самостоятельная работа по теме 2.2 (5 час.): Практическое задание «Аудит сетевой инфраструктуры»
Тема 2.3 Защита от атак методами социальной инженерии (7 час.)
Содержание темы Классификация атак и их характеристики. Выявление признаков неправомерного воздействия на пользователей информационных систем. Криминально-психологические приемы злоумышленников. Формирование устойчивости к эмоционально-волевым методам и манипулированию сознанием.
Самостоятельная работа по теме 2.3 (5 час.): Практическое задание «Выявление признаков социальной инженерии»
Тема 2.4 Защита персональных данных в цифровой среде (12 час.)
Содержание темы: Источники угроз и каналы утечки информации. Правовые основания. Права субъекта персональных данных. Обязанности оператора персональных данных. Ответственность за нарушения для физических лиц и для организаций. Последствия реализации угроз. Порядок реагирования на нарушения.
Самостоятельная работа по теме 2.4 (6 час.): Практическое задание «Выявление источников утечек персональных данных»

Описание практико-ориентированных заданий и кейсов

Номер темы/модуля	**Наименование практического занятия**	**Описание**
Модуль 1.	**Кибербезопасность в условиях цифровой экономики**	
1.1	Анализ угроз	Проанализируйте кейс и опишите реализованные угрозы и модель нарушителя.
1.2	Выявление требований к защищенности ИС	Классифицируйте используемую ИС по уровню защищенности согласно критериям ФСТЭК.
1.3	Подбор СЗИ	На основе предыдущего задания подберите не менее 3-х СЗИ, обеспечивающих нейтрализацию угроз ИС для соответствующего уровня защищенности.

Номер темы/модуля	Наименование практического занятия	Описание
Модуль 2.	**Защита от угроз и конфиденциальность**	
2.1	Конфигурирование антивирусного ПО	Установите и сконфигурируйте средство антивирусной защиты (на выбор).
2.2	Аудит сетевой инфраструктуры	Проведите аудит сетевой инфраструктуры с помощью инструментальных средств
2.3	Выявление признаков социальной инженерии	Проанализируйте кейс и выявите признаки атаки социальной инженерии, классифицируйте их и предложите алгоритм корректных действий для нейтрализации ситуации.
2.4	Выявление источников утечек персональных данных	Проанализируйте с помощью методологии OSINT открытые источники на предмет выявления утечек собственных персональных данных.

8. Оценочные материалы по образовательной программе

8.1. Вопросы аттестации

Вопросы входного тестирования	Вопросы промежуточного тестирования	Вопросы итогового тестирования
1) В какой ситуации целесообразно не предпринимать никаких мер по отношению к выявленным угрозам? a) Когда реализация необходимых в данной ситуации мер слишком сложна технически b) Когда стоимость мер по защите превышает ущерб от потери защищаемой информации c) Оба варианта верны 2) Как отличить легитимное приложение от вредоносного ПО с фишинговым функционалом для мобильной платформы Android? a) При установке приложения проверить все запрашиваемые разрешения (на доступ к смс-сообщениям, данным других приложений и т.д.) b) Устанавливать приложения только из Google Play c) По специальному значку на иконке легитимного приложения d) Верны варианты a и b. e) Верны варианты a и c. 3) Файерволлы для ПК и ноутбуков являются a) Исключительно программными. b) Программно-аппаратными комплексами c) Разрабатываются исключительно внешними (по отношению к ОС) разработчиками ПО. d) Всегда предустановлены разработчиками в защищаемую ОС 4) Невозможность получения сервиса законным пользователем называется a) Replay-атакой b) Spoofing-атакой c) DoS-атакой d) Атакой «man-in-the-middle»	Промежуточная аттестация по модулям не предусмотрена	1) Контроль за соблюдением правил защиты персональных данных осуществляется: Отметьте все подходящие варианты. a) ФСТЭК b) Роскомнадзор c) МВД 2) Какой способ двухфакторной авторизации наиболее устойчив к атакам злоумышленников: a) Одноразовые пароли, рассылаемые в смс-сообщениях b) Одноразовые коды, генерируемые приложениями-аутетинтификаторами (Google Authenticator, Authy) c) Второй постоянный пароль d) Все способы надежны в равной степени 3) Как называется атака, заключающаяся в использовании поддельной страницы веб-ресурса, созданной с целью сбора логинов, паролей и иных персональных данных пользователей? a) Фишинг b) Спуффинг c) DDoS d) DoS e) Man-in-the-Middle 4) Чтобы однократно воспользоваться определенным интернет-сервисом, требуется указать электронную почту. Какой адрес электронной почты следует указать? a) Рабочий b) Свой обычный адрес c) Воспользоваться сервисом алиасов 5) Сайт при регистрации потребовал ввести пароль с повышенными требованиями по длине и набору алфавита. Каким образом рекомендуется его запомнить?

Вопросы входного тестирования	Вопросы промежуточного тестирования	Вопросы итогового тестирования
5) Основной защитной мерой против атак «социальной инженерии» является a) повышение надежности криптографических алгоритмов b) работа по повышению уровню подготовки персонала c) страхование информационных ресурсов		a) Записать в телефон b) Записать на бумаге и спрятать её c) Сохранить в текстовом файле на компьютере d) Использовать специальные программы для хранения паролей в зашифрованном виде.

8.2. Описание показателей и критериев оценивания, шкалы оценивания.

На этапе входного контроля применяется измерительная шкала оценивания.

Критерий оценки	Показатели оценки					
	0	1	2	3	4	5
% правильных ответов	0-19	≥20	≥40	≥60	≥70	≥85

По кейс-задачам применяется аналитическая шкала оценивания:

Балл	Критерии оценивания
5	Обучающийся демонстрирует полное понимание проблемы. Все требования, предъявляемые к заданию, выполнены. Обучающийся самостоятельно, используя инструменты цифрового маркетинга, решил представленную практическую задачу применительно к своей компании или к виртуальной компании.
4	Обучающийся демонстрирует значительное понимание проблемы. Все требования, предъявляемые к заданию, выполнены. При выполнении задания допущены незначительные неточности.
3	Демонстрирует частичное понимание проблемы. Большинство требований, предъявляемых к заданию, выполнены. При выполнении задания требовалась значительная помощь преподавателя.
2	Демонстрирует небольшое понимание проблемы, задание выполнено частично.
1	Демонстрирует непонимание проблемы. Попытки выполнения задания были неверными.
0	Нет ответа. Не было попытки решить поставленную практическую задачу.

На этапе итоговой аттестации применяется измерительная шкала оценивания сформированности компетенций.

Критерий оценки	Показатели оценки					
	0	1	2	3	4	5
% правильных ответов	0-19	≥20	≥40	≥60	≥70	≥85

8.3. Примеры контрольных заданий по модулям или всей образовательной программе.

*Пример аналитического задания **по модулю 1**:*

Исходя из требуемого класса защищенности информационной системы подобрать конкретные средства защиты информации (СЗИ), реализующие ту или иную меру из для данного класса в соответствии с Приказом ФСТЭК №17 от 11.02.2013 г. Обоснуйте эффективность применения данных СЗИ для нейтрализации соответствующей угрозы.

*Пример аналитического задания **по модулю 2**:*

Пользуясь ресурсами сети Интернет, найти описание 3-х эпизодов кибератак с применением методов социальной инженерии (фишинг, троянский конь, и т.п.). Опишите эти эпизоды в файле и укажите источники. Проанализируйте один из эпизодов и ответьте на вопросы: Кто (в соответствии с моделью нарушителя) и с какой конечной целью производил атаку? Какие метод(ы) использовал злоумышленник (фишинг, троянский конь, дорожное яблоко, кви про кво, претекстинг, обратная социальная инженерия)? По каким признакам жертва могла выявить атаку? Какой комплекс мероприятий необходимо произвести, чтобы снизит вероятность реализации подобной атаки в будущем?

8.4. Тесты и обучающие задачи (кейсы), иные практикоориентированные формы заданий.

Модуль 1.

Пример тестового задания:

Какая категория лиц обладают наибольшим потенциалом реализации угроз информационной безопасности?

a) Хакеры
b) Контрагенты организации
c) Обслуживающий персонал
d) Сотрудники организации

Пример кейс-задачи:

Во время пребывания в помещении выставочного комплекса поступила личная просьба от знакомого перевести деньги на карту. Для этого планируется использовать мобильное банковское приложение. Что рекомендуется при этом сделать?

a) Т.к. просьба была сделана лично, а мобильное приложение банка легитимное, то дополнительных рисков нет. Можно сразу осуществить перевод.

b) Проверить, к какой сети подключено мобильное устройство, и если это общедоступная Wi-Fi сеть, то попросить персонал выдать данные для подключения к зашифрованной WI-FI сети и осуществлять перевод, только подключившись к ней.

c) Проверить, к какой сети подключено мобильное устройство, и если это общедоступная Wi-Fi сеть, то переключиться на мобильный интернет и только после этого осуществлять перевод.

Модуль 2.

Пример тестового задания:

Какой недостаток VPN сервисов является наиболее важным с точки зрения защиты информации?

a) Вероятность нарушения целостности информации
b) Вероятность нарушения конфиденциальности информации
c) Вероятность нарушения доступности информации*Пример кейс-задачи:*

При попытке разблокировать мобильное устройство на базе iOS возникает сообщение следующего содержания «Ваш телефон заблокирован. Для разблокирования пополните на 5000 рублей кошелек Яндекс деньги с номером….». Каким образом была совершена атака и как вести себя в этой ситуации?

a) Атака была совершена путем подбора (при использовании пароля, не удовлетворяющего требованиям безопасности) или перехвата пароля (при его вводе на фишинговых сайтах) от Apple-ID с последующей активацией функции «Найти Iphone» Необходимо обратиться в службу поддержки производителя устройства и предоставить ему данные, подтверждающие факт правомерного обладания устройством для осуществления разблокировки и возврата контроля над учетной записью.

b) Атака была совершена путем установки приложения с вредоносным функционалом из Appstore. Для разблокировки произвести оплату, т.к. иных способов вернуть контроль над устройством нет.

c) Атака была совершена путем эксплуатации уязвимостей протокола SS7, который позволил злоумышленнику получить полный удаленный контроль над устройством. Необходимо обратиться в службу поддержки производителя устройства и предоставить ему данные, подтверждающие факт правомерного обладания устройством для осуществления разблокировки и возврата контроля над учетной записью

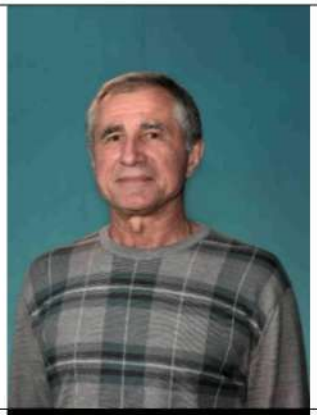
8.5. Описание процедуры оценивания результатов обучения.

Процедура оценивания результатов обучения зависит от типа оценочных материалов. Для тестов с множественным выбором предусмотрено автоматическое оценивание результатов. Для кейс-заданий, тестовых заданий в форме короткого ответа и эссе, аналитических заданий применяется метод ручного оценивания. Разрешено 2 попытки прохождения задания. В качестве результата засчитывается высшая из двух полученных оценок.

Входное и итоговое аттестационные испытания включают тестовые задания с вопросами только закрытого типа.

9. Организационно-педагогические условия реализации программы

9.1. Кадровое обеспечение программы

№ п/п	Фамилия, имя, отчество (при наличии)	Место основной работы и должность, ученая степень и ученое звание (при наличии)	Ссылки на веб-страницы с портфолио (при наличии)	Фото в формате jpeg	Отметка о полученном согласии на обработку персональных данных
1	Серпенинов Олег Витальевич	к.т.н., доцент кафедры Информационных технологий и защиты информации РГЭУ (РИНХ)	отсутствует		Согласен на обработку персональных данных
2	Назарян Сергей Ашотович	старший преподаватель кафедры Информационных технологий и защиты информации РГЭУ (РИНХ)	отсутствует		Согласен на обработку персональных данных
3	Прохоров Антон Игоревич	старший преподаватель кафедры Информационных технологий и защиты информации РГЭУ (РИНХ), сертифицированный инструктор Сетевой академии Cisco	отсутствует		Согласен на обработку персональных данных

9.2. Учебно-методическое обеспечение и информационное сопровождение

Учебно-методические материалы	
Методы, формы и технологии	**Методические разработки, материалы курса, учебная литература**
- лекции в форме вебинаров - тест	Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
	Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных».
	Доктрина информационной безопасности Российской Федерации. Утверждена указом Президента Российской Федерации 05.12.2016 No646
	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15.02.2008.

Учебно-методические материалы	
Методы, формы и технологии	**Методические разработки, материалы курса, учебная литература**
	Масалков А.С. Особенности киберпреступлений. Инструменты нападения и защита информации / А.С.Масалков; ДМК Пресс. –Москва. 2018, - 226 с.- ISBN: 978-5-97060- 651-3
	Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. : схем., табл., ил. - Библиогр. в кн. - ISBN 978-5-9275-2364-1
	Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом : учебное пособие / Н.Б. Ельчанинова ; Министерство науки и высшего образования РФ, Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет», Инженерно-технологическая академия. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2017. - 77 с. - Библиогр. в кн. - ISBN 978-5-9275-2501-0
	Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7
	Защита персональных данных в информационных системах : лабораторный практикум / авт.-сост. В.И. Петренко, И.В. Мандрица ; Министерство образования и науки Российской Федерации, Северо-Кавказский федеральный университет. - Ставрополь : СКФУ, 2018. - 118 с.
	Смирнов, В.И. Защита информации : лабораторный практикум / В.И. Смирнов ; Поволжский государственный технологический университет. - Йошкар-Ола : ПГТУ, 2017. - 67 с. : ил. - Библиогр. в кн. - ISBN 978-5-8158-1866-8

Информационное сопровождение	
Электронные образовательные ресурсы	Электронные информационные ресурсы
Электронный учебно-методический комплекс образовательной программы размещен на портале электронного обучения РГЭУ (РИНХ)– Режим доступа: https://do.rsue.ru	Официальный сайт ФСТЭК России – URL: http://fstec.ru.
	Банк данных угроз безопасности информации – URL: http://bdu.fstec.ru. /
	Портал персональных данных Уполномоченного органа по защите прав субъектов персональных данных – URL: http://pd.rkn.gov.ru.

9.3. Материально-технические условия реализации программы

Вид занятий	Наименование оборудования, программного обеспечения
Лекция	ПЭВМ под управлением операционной системы Microsoft Windows, Linux либо MacOS с установленным веб-браузером (Google Chrome/Mozilla Firefox/Safari/Opera/Яндекс.Браузер/Atom), программа для видеоконференций Zoom..
Самостоятельная работа	

II. **Паспорт компетенций** (Приложение 2)

Приложение 2

ФГБОУ ВО «Ростовский государственный экономический университет (РИНХ)»

ПАСПОРТ КОМПЕТЕНЦИИ

Дополнительная профессиональная программа – программа повышения квалификации «Основы личной и корпоративной кибербезопасности в цифровой экономике»

<table>
<tr><td>1.</td><td>Наименование компетенции</td><td colspan="2">Способность осуществлять защиту устройств и цифрового контента</td></tr>
<tr><td>2.</td><td>Указание типа компетенции</td><td colspan="2">профессиональная</td></tr>
<tr><td>3.</td><td>Определение, содержание и основные сущностные характеристики компетенции</td><td colspan="2">Под компетенцией понимается способность осуществлять защиту устройств и цифрового контента в условиях существования угроз безопасности информации путем реализации комплекса правовых, организационных и программно-технических мер

Слушатель должен:
знать:
актуальную законодательную и нормативную правовую базу, обеспечивающие реализацию мер по защите информации; основные виды угроз безопасности информации в информационных системах; содержание и порядок организации работ по выявлению угроз безопасности информации в информационных системах; методы и средства обеспечения кибербезопасности
уметь:
планировать мероприятия по обеспечению кибербезопасности; выявлять потенциальные риски и оценивать угрозы безопасности информации в цифровых средах; определять требования к защищённости информационных систем в зависимости от характера угроз; подбирать и применять методы и средства защиты информации, наиболее релевантные требованиям к защищенности
владеть:
навыками реализации положений законодательной базы и нормативных правовых актов в области обеспечения кибербезопасности; обеспечения антивирусной защиты устройств, в т.ч. портативных, выявления и нейтрализации вредоносных программ; выявление угроз и обеспечение безопасности данных, передаваемых по сети Интернет, в т.ч. по беспроводным каналам; выявления криминально-психологических методов воздействия на пользователя информационных систем и обеспечение устойчивости к кибератакам методами социальной инженерии</td></tr>
<tr><td rowspan="3">4.</td><td rowspan="3">Дескриптор знаний, умений и навыков по уровням</td><td>Уровни сформированности компетенции обучающегося</td><td>Индикаторы</td></tr>
<tr><td>Начальный уровень

(Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.)</td><td>Знает: базовый понятийный аппарат и наиболее обшие положения законодательства о защите информации, отдельные угрозы
Умеет: применять отдельные средства обеспечения кибербезопасности
Владеет: навыками выявления отдельных видов угроз</td></tr>
<tr><td>Базовый уровень

(Уверенно владеет навыками, способен, проявлять соответствующие навыки в</td><td>Знает: понятийный аппарат и отдельные положения законодательства о защите информации, классификацию угроз.
Умеет: применять базовые средства обеспечения информационной</td></tr>
</table>

		ситуациях с элементами неопределённости, сложности.)	безопасности Владеет: навыками выявления угрозы кибербезопасности, включая угрозы социальной инженерии.
		Продвинутый (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.)	Знает: понятийный аппарат; актуальную законодательную и нормативную правовую базу, обеспечивающие реализацию мер по защите информации Умеет: применять широкий набор средств обеспечения кибербезопасности, Владеет: навыками выявления угроз кибербезопасности с помощью инструментальных средств
		Профессиональный (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействующими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.)	Знает: актуальную законодательную и нормативную правовую базу, обеспечивающие реализацию мер по защите информации; основные виды угроз безопасности информации в информационных системах; содержание и порядок организации работ по выявлению угроз безопасности информации в информационных системах; методы и средства обеспечения кибербезопасности Умеет: планировать мероприятия по обеспечению кибербезопасности; выявлять потенциальные риски и оценивать угрозы безопасности информации в цифровых средах; определять требования к защищённости информационных систем в зависимости от характера угроз; подбирать и применять методы и средства защиты информации, наиболее релевантные требованиям к защищенности Владеет: навыками реализации положений законодательной базы и нормативных правовых актов в области обеспечения кибербезопасности; обеспечения антивирусной защиты устройств, в т.ч. портативных, выявления и нейтрализации вредоносных программ; выявление угроз и обеспечение безопасности данных, передаваемых по сети Интернет, в т.ч. по беспроводным каналам; выявления криминально-психологических методов воздействия на пользователя информационных систем и обеспечение устойчивости к кибератакам методами социальной инженерии
5.	Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции	Владение данной компетенцией является необходимым условием для овладения компетенцией «способность обеспечивать конфиденциальность и защиту персональных данных»	
6.	Средства и технологии оценки	Тесты	

ПАСПОРТ КОМПЕТЕНЦИИ

Дополнительная профессиональная программа – программа повышения квалификации «Основы личной и корпоративной кибербезопасности в цифровой экономике»

<table>
<tr><td>1</td><td>Наименование компетенции</td><td colspan="2">способностью обеспечить конфиденциальность персональных данных при взаимодействии с различными информационными системами и ресурсами</td></tr>
<tr><td>2</td><td>Указание типа компетенции</td><td colspan="2">профессиональная</td></tr>
<tr><td>3</td><td>Определение, содержание и основные сущностные характеристики компетенции</td><td colspan="2">Под компетенцией понимается способность выявлять угрозы, ведущие к утечке персональных данных, оценивать их последствия и подбирать и применять релевантный набор средств нейтрализации и защиты.
Слушатель должен:
знать:
актуальная законодательная и нормативная правовая база, обеспечивающие реализацию мер по защите персональных данных, включая права и обязанности субъектов и операторов персональных данных, положения юридической ответственности за нарушения законодательства о персональных данных; содержание и порядок организации работ по выявлению угроз безопасности персональных данных информации в информационных системах
знания о методах и средствах обеспечения безопасности персональных данных
уметь:
выявлять потенциальные риски и оценивать угрозы безопасности информации в цифровых средах, в т.ч. персональных данных; определять требования к защищённости информационных систем, в т.ч. информационных систем персональных данных подбирать и применять методы, инструменты и средства защиты информации, наиболее релевантные требованиям к защищенности
владеть:
навыками реализации положений законодательной базы и нормативных правовых актов в области обеспечения безопасности персональных данных на уровне субъекта и оператора персональных данных; навыками обеспечения защиты устройств от утечек персональных данных;
выявлению угроз и обеспечение безопасности данных, передаваемых по сети Интернет, в т.ч. по беспроводным каналам; выявление криминально-психологических методов воздействия на пользователя информационных систем и обеспечение устойчивости к кибератакам методами социальной инженерии; выявления утечек персональных данных с помощью инструментария методологии OSINT.предотвращение утечки персональных данных и их защите в информационных системах/</td></tr>
<tr><td>$ 4</td><td>Дескриптор знаний, умений и навыков по уровням</td><td>Уровни сформированности компетенции обучающегося</td><td>Индикаторы</td></tr>
<tr><td></td><td></td><td>Начальный уровень

(Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.)</td><td>Знает: понятийный аппарат в области защиты персональных данных
Умеет: конфигурировать базовые инструменты защиты персональных данных личных устройств
Владеет: навыками выявления признаков отдельных угроз</td></tr>
<tr><td></td><td></td><td>Базовый уровень

(Уверенно владеет навыками, способен, проявлять соответствующие навыки в</td><td>Знает: положения законодательства о защите персональные данных, включая права и обязанности субъектов и операторов персональных данных
Умеет: обеспечивать безопасность</td></tr>
</table>

		ситуациях с элементами неопределён-ности, сложности.)	персональных данных на личных устройствах Владеет: навыками выявления угроз персональным данным с помощью инструментальных средств
		Продвинутый (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.)	Знает: актуальную нормативную и правовую базу, включая положения документов ФСТЭК и Роскомнадзора. Умеет: реализовывать комплекс мер по защите персональных данных в рамках АРМ и персональных устройств. Владеет: навыками оценки безопасности и выявления утечек персональных данных с помощью инструментальных средств
		Профессиональный (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействующими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.)	Знает: актуальную законодательная и нормативную правовая база, обеспечивающие реализацию мер по защите персональных данных, включая права и обязанности субъектов и операторов персональных данных, положения юридической ответственности за нарушения законодательства о персональных данных; содержание и порядок организации работ по выявлению угроз безопасности персональных данных информации в информационных системах Умеет:выявлять потенциальные риски и оценивать угрозы безопасности информации в цифровых средах, в т.ч. персональных данных; определять требования к защищённости информационных систем, в т.ч. информационных систем персональных данных подбирать и применять методы, инструменты и средства защиты информации, наиболее релевантные требованиям к защищенности Владеет:навыками реализации положений законодательной базы и нормативных правовых актов в области обеспечения безопасности персональных данных на уровне субъекта и оператора персональных данных; навыками обеспечения защиты устройств от утечек персональных данных; выявлению угроз и обеспечение безопасности данных, передаваемых по сети Интернет, в т.ч. по беспроводным каналам; выявление криминально-психологических методов воздействия на пользователя информационных систем и обеспечение устойчивости к кибератакам методами социальной инженерии; выявления утечек персональных данных с помощью инструментария методологии OSINT.предотвращение утечки персональных данных и их защите в информационных системах
	Характеристика взаимосвязи данной компетенции с другими компетенциями/	Для овладения данной компетенцией требуется овладения компетенцией «способность осуществлять защиту устройств и цифрового контента»	

	необходимость владения другими компетенциями для формирования данной компетенции	
	Средства и технологии оценки	Тесты

VI. Иная информация о качестве и востребованности образовательной программы
Настоящая образовательная программа основана на материалах образовательной программы "Кибербезопасность в цифровой экономике", успешно апробированной в рамках пилотного проекта программы персональных цифровых сертификатов.

V. Рекомендаций к программе от работодателей: Имеются 2 письма- рекомендации от ООО «Дон-Фин-Аудит» и ООО «Логос».

VI. Указание на возможные сценарии профессиональной траектории граждан по итогам освоения образовательной программы

Текущий статус	Цель
освоение смежных профессиональных областей	повышение уровня дохода, расширение профессиональной деятельности
работающий по найму в организации, на предприятии	развитие профессиональных качеств
	повышение заработной платы

VII.Дополнительная информация - отсутствует
VIII.Приложенные Скан-копии - Утвержденная образовательная программа

СОГЛАСОВАНО:

Проректор
по развитию образовательных программ Т.В. Торопова

Директор Бизнес-школы О.Н. Степаненко