Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)
Колледж информатики и программирования

УТВЕРЖДАЮ

Заместитель директора по
учебной работе

_____ Н.Ю. Долгова
«__30__» ____июня____2022г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Москва 2022г.

Рабочая программа учебный дисциплины разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

(код и наименование специальности)

Разработчики:
Поколодина Елена Владиславна, к.э.н., преподаватель 1КК Колледжа информатики и программирования, Володин Сергей Михайлович, к.т.н., преподаватель ВКК Колледжа информатики и программирования, Маринич Анна Леонидовна, преподаватель 1КК Колледжа информатики и программирования

Рецензент:
Эдгулова Елизавета Каральбиевна, кандидат физико – математических наук, преподаватель колледжа информационных технологий и экономики КБГУ

(ФИО, ученая степень, звание, должность)

Рабочая программа учебной дисциплины рассмотрена и рекомендована к утверждению на заседании предметной (цикловой) комиссии Обеспечения информационной безопасности автоматизированных систем

Протокол от «12» 05 2022 г. № 10

Председатель ПЦК _____ С.М. Володин
(подпись)

Р Е Ц Е Н З И Я

на рабочую программу дисциплины ОП. 01 «Основы информационной безопасности», составленную Поколодиной Е. В., к.э.н., преподаватель 1КК Колледжа информатики и программирования, Володиным С. М., к.т.н., преподаватель ВКК Колледжа информатики и программирования, Маринич А. Л., преподаватель 1КК Колледжа информатики и программирования

Рабочая программа дисциплины «Основы информационной безопасности» включает в себя **60 часов,** из которых **18 часов** отводится на практические работы.

Содержание данной программы направлено на формирование у выпускника следующих компетенций: ОК 03, ОК 06, ОК 09, ОК 10, ПК.2.4

Структура учебной дисциплины, в частности распределение учебных часов между практическими и самостоятельными занятиями, направлена на закрепление знаний, полученных на теоретических занятиях. Тематический план и содержание учебной дисциплины обеспечивает соответствие требованиям ФГОС по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» к знаниям, умениям, практическому опыту, а именно:

уметь:
классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
классифицировать основные угрозы безопасности информации;
регистрировать и анализировать события, выявлять признаки атак и инцидентов информационной безопасности (06.033 А/2.05).

знать:
сущность и понятие информационной безопасности, характеристику ее составляющих (06.032 А/1.05, А/2.05);
место информационной безопасности в системе национальной безопасности страны (06.032 А/1.05, А/2.05);
источники угроз информационной безопасности и меры по их предотвращению;
жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
современные способы, методы и средства обеспечения информационной безопасности;
основные методики анализа угроз и рисков информационной безопасности.

В рабочей программе большое внимание уделяется классификации информации по видам, классификации информационных угроз, прикладным возможностям защиты и отражения различных видов атак и несанкционированных посягательств на информацию.

В целом предлагаемая рабочая программа дисциплины «Основы информационной безопасности» является достаточной и соответствующей требованиям Федерального государственного образовательного стандарта по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем». Программа может быть использована в учреждениях СПО для подготовки выпускников данной специальности.

Рецензент: Эдгулова Елизавета Каральбиевна
кандидат физико-математических наук, председатель Цикловой комиссии информационных технологий и программирования, преподаватель колледжа информационных технологий и экономики КБГУ

(Фамилия И.О., должность, ученая степень, ученое звание, подпись)

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ 4
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ 7
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ 11
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ 14

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Место дисциплины в структуре основной образовательной программы

Учебная дисциплина «Основы информационной безопасности» является обязательной частью цикла основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Учебная дисциплина «Основы информационной безопасности» обеспечивает формирование профессиональных и общих компетенций по всем видам деятельности ФГОС специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Особое значение дисциплина имеет при формировании и развитии общих, профессиональных компетенций и личностных результатов.

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках

1.1.2. Перечень профессиональных компетенций

Код	Наименование профессиональных компетенций
ПК 2.4	Осуществлять обработку, хранение и передачу информации ограниченного доступа

1.1.3. Перечень личностных результатов

Код	Наименование личностных результатов
ЛР 1	Осознающий себя гражданином и защитником великой страны
ЛР 3	Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих

ЛР 4	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
ЛР 10	Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой
ЛР 13	Демонстрирующий готовность и способность вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения в профессиональной деятельности
ЛР 14	Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности
ЛР 15	Проявляющий гражданское отношение к профессиональной деятельности как к возможности личного участия в решении общественных, государственных, общенациональных проблем
ЛР 18	Демонстрирующий способность использовать в цифровой среде различные цифровые средства, позволяющие во взаимодействии с другими людьми достигать поставленных целей; предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве.

1.2.Цель и планируемые результаты освоения дисциплины:

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ОК, ПК	Умения	Знания
ОК 03 ОК06 ОК 09 ОК10 ПК 2.4.	- классифицировать защищаемую информацию по видам тайны и степеням секретности; - классифицировать основные угрозы безопасности информации.	- сущность и понятие информационной безопасности, характеристику ее составляющих; - место информационной безопасности в системе национальной безопасности страны; - виды, источники и носители защищаемой информации; - источники угроз безопасности информации и меры по их предотвращению; - факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; - жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; - современные средства и способы обеспечения информационной безопасности; - основные методики анализа угроз и рисков информационной безопасности.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем в часах/ в том числе в форме практической подготовки [1]
Объем образовательной программы учебной дисциплины	60/18
Объем работы обучающихся во взаимодействии с преподавателем	60/18
в том числе:	
теоретическое обучение/*в том числе в форме практической подготовки*	30/0
практические занятия/ *в том числе в форме практической подготовки*	18/18
лабораторные работы / *в том числе в форме практической подготовки*	-
контрольные работы	-
самостоятельная работа/ *в том числе в форме практической подготовки*	-
Промежуточная аттестация в форме экзамена	12

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы. Коды личностных результатов, формированию которых реализации программы воспитания.
1	2	3	4
РАЗДЕЛ 1. Теоретические основы информационной безопасности		**28/10**	
Тема 1.1 Основные понятия и задачи информационной безопасности	**Содержание учебного материала**	4/0	ОК 06, ОК 09, ОК.10, ПК.2.4, ЛР1, ЛР2, ЛР3, ЛР4, ЛР10, ЛР13, ЛР14, ЛР 15, ЛР18
	1.Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.	2/0	
	2.Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности.	2/0	
Тема 1.2. Основы защиты информации	**Содержание учебного материала**	14/6	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4, ЛР1, ЛР2, ЛР3, ЛР4, ЛР10, ЛР13, ЛР14, ЛР 15, ЛР18
	1. Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации	2/0	
	2.Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.	2/0	
	3.Цели и задачи защиты информации. Основные понятия в области защиты информации.	2/0	

	4.Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.	2/0	
	В том числе практических занятий	6/6	
	1. Практическое занятие «Определение объектов защиты на типовом объекте информатизации».	2/2	
	2. Практическое занятие «Классификация защищаемой информации по видам тайны и степеням конфиденциальности».	4/4	
Тема 1.3. Угрозы безопасности защищаемой информации.	**Содержание учебного материала**	10/4	
	1.Понятие угрозы безопасности информации	6/0	ОК 03, ОК 06, ОК 09, ПК.2.4, ЛР1, ЛР2, ЛР3, ЛР4, ЛР10, ЛР13, ЛР14, ЛР 15, ЛР18
	2.Системная классификация угроз безопасности информации.		
	3.Каналы и методы несанкционированного доступа к информации		
	4.Уязвимости. Методы оценки уязвимости информации		
	В том числе практических занятий	4/4	
	3. Практическое занятие «Определение угроз объекта информатизации и их классификация».	4/4	
РАЗДЕЛ 2. Методология защиты информации		**20/8**	
Тема 2.1. Методологические подходы к защите информации	Содержание учебного материала	4/0	ОК 03, ОК 06, ОК 09, ПК 2.4, ЛР1, ЛР2, ЛР3, ЛР4, ЛР10, ЛР13, ЛР14, ЛР 15, ЛР18
	1. Анализ существующих методик определения требований к защите информации.	2/0	
	2. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.	2/0	
	3. Виды мер и основные принципы защиты информации.		
Тема 2.2. Нормативно правовое регулирование защиты информации	Содержание учебного материала	8/4	ОК 03, ОК 06, ОК 09, ОК 10, ЛР1, ЛР2, ЛР3, ЛР4, ЛР10, ЛР13, ЛР14, ЛР 15, ЛР18
	1.Организационная структура системы защиты информации	2/0	
	2.Законодательные акты в области защиты информации.		
	3.Российские и международные стандарты, определяющие требования к защите информации.	2/0	

	4. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации		
	В том числе практических занятий	4/4	
	4.Практическое занятие «Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности».	4/4	
Тема 2.3. Защита информации в автоматизированных (информационных) системах	Содержание учебного материала	8/4	ОК 03, ОК 06, ОК 09, ОК 10, ЛР1, ЛР2, ЛР3, ЛР4, ЛР10, ЛР13, ЛР14, ЛР 15, ЛР18
	1.Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.	2/0	
	2.Программные и программно-аппаратные средства защиты информации		
	3.Инженерная защита и техническая охрана объектов информатизации	2/0	
	4.Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.		
	В том числе практических занятий	4/4	
	5.Практическое занятие «Выбор мер защиты информации для автоматизированного рабочего места».	4/4	
Промежуточная аттестация в форме экзамена		12	
Всего:		60/18	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Реализация программы дисциплины требует наличия учебного кабинета информационной безопасности, лаборатории информационных технологий (в соответствии с ФГОС и ПООП):

Специализированная мебель:

Стол студенческий одноместный – 26 шт.

Стулья компьютерные – 26 шт.

Стол (учительский) – 1 шт.

Стул (учительский) – 1 шт.

Доска (меловая) – 1 шт.

Технические средства обучения:

Компьютер студенческий – 25 шт.

Компьютер преподавателя – 1 шт.

Лицензионное программное обеспечение общего и профессионального назначения

Компьютеры подключены к локальной вычислительной сети, информационно-образовательной среде Финуниверситета и сети Интернет

Учебно-наглядные и методические пособия, учебно-методическая документация.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемых для использования в образовательном процессе

3.2.1. Печатные издания

Основная литература:

1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2022. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст: электронный //

Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495524

2. Суворова, Г. *М.* Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741

3.2.2. Электронные издания (электронные ресурсы)

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2022. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495525

2. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниязов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва: Издательство Юрайт, 2022. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498889

3. Национальный открытый университет ИНТУИТ, курс "Основы информационной безопасности". URL: http://www.intuit.ru/studies/courses/10/10/info

5. ФСТЭК России. Методические указания, НМД. URL: http://fstec.ru/component/tags/tag/11-metodicheskij-dokument

6. Аналитика по информационной безопасности Positive Technologies/URL: http://www.ptsecurity.ru/research

7. Образовательные порталы по различным направлениям образования и тематик URL: https://edu.garant.ru/education/references/portal/

8. Информационный портал по безопасности компании Positive Technologies URL: www.securitylab.ru/

9. ИТ-портал компании "Инфосистемы Джет". URL: http://www.jetinfo.ru

10. Научно-практический журнал «Вопросы кибербезопасности». URL: http://cyberrus.com/

11. Научно-практический журнал «Безопасность информационных технологий». URL: http://bit.mephi.ru/

12. Справочно-правовая система «Консультант Плюс» www.consultant.ru

14. Федеральный портал «Российское образование www.edu.ru

15. Федеральный правовой портал «Юридическая Россия» www.law.edu.ru

16. Федеральный портал «Социально-гуманитарное и политологическое образование» www.humanities.edu.ru

17. Федеральный портал «Информационно- коммуникационные технологии в образовании» http://www.ict.edu.ru

18. Сайт Научной электронной библиотеки www.elibrary.ru

3.2.3. Дополнительные источники:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2022. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497433

2. Хрусталева, З.А., Метрология, стандартизация и сертификация. Практикум.: учебное пособие / З.А. Хрусталева. — Москва: КноРус, 2021. — 171 с. — ISBN 978-5-406-03241-1. — URL:https://book.ru/book/937033

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения	Критерии оценки	Методы оценки
Перечень знаний, осваиваемых в рамках дисциплины: – сущность и понятие информационной безопасности, характеристику ее составляющих; – место информационной безопасности в системе национальной безопасности страны; – виды, источники и носители защищаемой информации; – источники угроз безопасности информации и меры по их предотвращению; – факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; – жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; – современные средства и способы обеспечения информационной безопасности; – основные методики анализа угроз и рисков информационной безопасности.	«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Устные опросы; Наблюдение за ходом выполнения практических работ; Компьютерное тестирование на знание терминологии по теме; - Оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий. Оценка ответа на экзамене.
Перечень умений, осваиваемых в рамках дисциплины: – классифицировать защищаемую информацию по		

видам тайны и степеням секретности; – классифицировать основные угрозы безопасности информации.		