

**Автономная некоммерческая профессиональная
образовательная организация
«Тамбовский колледж бизнес-технологий»**

Рабочая программа учебной дисциплины

ОП.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

для специальности среднего профессионального образования

**10.02.05. Обеспечение информационной безопасности ав-
томатизированных систем**

на базе основного и среднего общего образования

**Тамбов
2022**

Разработана на основе:

- Федерального государственного образовательного стандарта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Одобрена

ПЦК информационных и математических дисциплин

Председатель ПЦК



/ Самсонов Д.Ю., к.э.н.

Подпись

ФИО

Составитель (автор): Оскаленко Д.А., к.т.н
ФИО, ученая степень

Содержание

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	4
1.1. Место дисциплины в структуре примерной основной профессиональной образовательной программы:	4
1.2. Цель и планируемые результаты освоения дисциплины:	4
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	6
2.1 Объем учебной дисциплины и виды учебной работы	6
2.2. Тематический план и содержание учебной дисциплины «Основы информационной безопасности»	7
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	11
3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:	11
3.2 Информационное обеспечение обучения.....	11
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ ..	12
5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ ПО ОСВОЕНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ ПРИ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОГО ОБУЧЕНИЯ И ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ.....	15

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Место дисциплины в структуре примерной основной профессиональной образовательной программы:

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности среднего профессионального образования 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Дисциплина *ОП.01 Основы информационной безопасности* входит в общепрофессиональный цикл, является дисциплиной, дающей начальные представления и понятия в области информационной безопасности, определяющей потребности в развитии интереса к изучению учебных дисциплин и профессиональных модулей, способности к личному самоопределению и самореализации в учебной деятельности.

Особое значение дисциплина имеет при формировании и развитии: ОК 0.3, ОК 06, ОК 09, ОК 10, ПК 2.4

Рабочая программа разработана на основании Положения о разработке рабочих программ учебных дисциплин по специальностям СПО, утвержденного приказом директора от 12.07.2017 года и Распоряжения об актуализации учебно-методических материалов, связанных с дистанционным обучением студентов, утвержденного приказом директора от 06.04.2020 года.

Изучение учебной дисциплины «Основы алгоритмизации и программирования» обучающимися с ограниченными возможностями здоровья осуществляется в соответствии с Приказом Министерства образования и науки РФ от 9 ноября 2015 г. № 1309 «Об утверждении Порядка обеспечения условий доступности для инвалидов объектов и предоставляемых услуг в сфере образования, а также оказания им при этом необходимой помощи», Положением о порядке обучения обучающихся – инвалидов и лиц с ограниченными возможностями здоровья, утвержденным директором от 12.07.2017. Предоставление специальных технических средств обучения коллективного и индивидуального пользования, подбор и разработка учебных материалов для обучающихся с ограниченными возможностями здоровья производится преподавателями с учетом индивидуальных психофизиологических особенностей обучающихся и специфики приема-передачи учебной информации. С обучающимися по индивидуальному плану и индивидуальному графику проводятся индивидуальные занятия и консультации.

1.2. Цель и планируемые результаты освоения дисциплины:

Код ПК, ОК	Умения	Знания
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие. ОК 06. Проявлять	классифицировать защищаемую информацию по видам тайны и степеням секретности; классифицировать основные угрозы безопасности	сущность и понятие информационной безопасности, характеристику ее составляющих; место информационной безопасности в системе национальной безопасности страны;

<p>гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.</p> <p>ОК 09. Использовать информационные технологии в профессиональной деятельности.</p> <p>ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.</p> <p>ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.</p>	<p>информации;</p>	<p>виды, источники и носители защищаемой информации;</p> <p>источники угроз безопасности информации и меры по их предотвращению;</p> <p>факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;</p> <p>жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;</p> <p>современные средства и способы обеспечения информационной безопасности;</p> <p>основные методики анализа угроз и рисков информационной безопасности;</p>
--	--------------------	---

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов		
	всего	обязательная часть	вариативная часть
Максимальная учебная нагрузка (всего)	98	48	50
Обязательная аудиторная учебная нагрузка (всего)	80	30	50
в том числе:			
лекции	40	14	26
лабораторные занятия	-	-	-
практические занятия	40	16	24
контрольные работы	-	-	-
курсовая работа (проект) <i>не предусмотрена</i>	-	-	-
Самостоятельная работа обучающегося (всего)	-	-	-
в том числе:			
самостоятельная работа над индивидуальным проектом	-	-	-
Промежуточная аттестация в форме:			
- Экзамен (3 семестр),	18	18	

2.2. Тематический план и содержание учебной дисциплины «Основы информационной безопасности»

Наименование разделов и тем	Содержание учебного материала, практические работы, семинарские занятия, самостоятельная работа обучающихся	Объем часов	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Раздел 1. Теоретические основы информационной безопасности		42	
Тема 1.1. Основные понятия и задачи информационной безопасности	Содержание учебного материала	6	ОК 3, ОК 6, ОК 9, ОК 10 ПК.2.4
	Лекционные занятия:	6	
	Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.	2	
	Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий.	2	
	Сущность функционирования системы защиты информации. Защита человека от опасной информации и от не информированности в области информационной безопасности.	2	
Тема 1.2. Основы защиты информации	Содержание учебного материала	20	ОК 3, ОК 6, ОК 9, ОК 10 ПК.2.4
	Лекционные занятия:	10	
	Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности.	2	
	Понятия государственной тайны и конфиденциальной информации. Понятие политики безопасности.	2	
	Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.	2	
	Цели и задачи защиты информации. Основные понятия в области защиты информации.	2	
	Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности	2	

	в основную деятельность организации.		
	Практические занятия:	10	
	Определение уровня конфиденциальности информации на объекте информатизации.	2	
	Определение объектов защиты на типовом объекте информатизации.	2	
	Исследование жизненного цикла конфиденциальной информации в процессе ее создания, обработки, передачи.	2	
	Классификация защищаемой информации по видам тайны и степеням конфиденциальности.	2	
	Исследование моделей управления информационной безопасностью на объекте.	2	
Тема 1.3. Угрозы безопасности защищаемой информации.	Содержание учебного материала	16	ОК 3, ОК 6, ОК 9, ОК 10 ПК.2.4
	Лекционные занятия:	6	
	Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации.	2	
	Каналы и методы несанкционированного доступа (НСД) к информации.	2	
	Уязвимости. Методы оценки уязвимости информации.	2	
	Практические занятия:	10	
	Анализ угроз безопасности информации.	2	
	Построение модели угроз безопасности информации.	2	
	Определение каналов и методов НСД к информации на объекте.	2	
	Определение уровня уязвимостей на объекте информатизации.	2	
	Организация политики безопасности на объекте информатизации.	2	
Раздел 2. Методология защиты информации		38	
Тема 2.1. Методологические подходы к защите информации	Содержание учебного материала	6	ОК 3, ОК 6, ОК 9, ОК 10 ПК.2.4
	Лекционные занятия:	6	
	Анализ существующих методик определения требований к защите информации.	2	
	Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.	2	
	Виды мер и основные принципы защиты информации.	2	
Тема 2.2. Нормативно-	Содержание учебного материала	16	ОК 3, ОК 6, ОК

правовое регулирование защиты информации	Лекционные занятия:	6	9, ОК 10 ПК.2.4
	Организационная структура системы защиты информации. Законодательные акты в области защиты информации.	2	
	Российские и международные стандарты, определяющие требования к защите информации.	2	
	Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации.	2	
	Практические занятия:	10	
	Работа информационно-поисковых системах с законодательными актами в области защиты информации	2	
	Работа с российскими и международными стандартами в области защиты информации	2	
	Работа с методическим документом ФСТЭК России «Меры защиты информации в государственных информационных системах»	2	
	Работа с реестрами ФСТЭК России в области защиты информации	2	
	Изучение государственных отечественных стандартов (ГОСТ) в области сертификации средств информационной безопасности	2	
Тема 2.3. Защита информации в автоматизированных (информационных) системах	Содержание учебного материала	16	ОК 3, ОК 6, ОК 9, ОК 10 ПК.2.4
	Лекционные занятия:	6	
	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.	2	
	Программные и программно-аппаратные средства защиты информации. Инженерная защита и техническая охрана объектов информатизации	2	
	Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.	2	
	Практические занятия:	10	
	Выбор мер защиты информации для автоматизированного рабочего места.	2	
	Изучение программных и программно-аппаратных средств защиты информации.	2	
	Изучение инженерно-технических средств защиты информации.	2	
	Выбор режима доступа на объект информатизации и создание его организационной защиты.	2	

	Изучение методов работы и профилактики кадровых сотрудников в сфере информационной безопасности на объекте.	2	
<i>Промежуточная аттестация по учебной дисциплине Экзамен</i>		18	
Всего		98	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Реализация программы дисциплины требует наличия компьютерного класса (ауд. 203)

Оборудование учебного кабинета: персональный компьютер, проектор, презентации уроков, стенды, плакаты, методические пособия.

Оборудование лаборатории информационных технологий: посадочные места по количеству обучающихся; рабочее место преподавателя; мультимедийное оборудование.

3.2 Информационное обеспечение обучения

3.2.1. Основные источники:

1. *Внуков, А. А.* Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с. — (Профессиональное образование). — ISBN 978-5-534-10711-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/456793>.
2. *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, 2020. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/456792>

3.2.2. Дополнительные источники

3. *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2020. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/543873>.

3.2.3 Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Федеральный портал «Российское образование» www.edu.ru
6. Федеральный правовой портал «Юридическая Россия» <http://www.law.edu.ru/>
7. Российский биометрический портал www.biometrics.ru
8. Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>
9. Сайт Научной электронной библиотеки www.elibrary.ru

3.2.4. Платформы, активно используемые для онлайн-связи в период вынужденного дистанционного обучения

1. Платформа для проведения онлайн-занятий ZOOM <https://zoom-us>.
2. Инструмент для связи с бесплатными звонками и чатами Skype <https://www.skype.com>
3. Платформа для проведения веб-конференций ЗСХ <https://tkbt.my3cx.ru/> · Мессенджер WhatsApp <https://www.whatsapp.com/>
4. VK мессенджер <https://vk.com/webkamera>

• **4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ**

Результаты обучения	Критерии оценки	Формы и методы оценки
<p>В результате освоения дисциплины обучающийся должен <i>знать</i>:</p> <p>сущность и понятие информационной безопасности, характеристику ее составляющих;</p> <p>место информационной безопасности в системе национальной безопасности страны;</p> <p>виды, источники и носители защищаемой информации;</p> <p>источники угроз безопасности информации и меры по их предотвращению;</p> <p>факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;</p> <p>жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;</p> <p>современные средства и способы обеспечения информационной безопасности;</p> <p>основные методики анализа угроз и рисков информационной безопасности.</p>	<p>Демонстрация знаний по курсу «Основы информационной безопасности» в повседневной и профессиональной деятельности.</p>	<p>Устный опрос, тестирование,</p> <p>Выполнение практических работ.</p> <p>Текущий и рубежный контроль, в т.ч.с применением ДОТ,</p> <p>выполнение контрольных заданий и итоговых тестов с применением ЭО.</p> <p>Промежуточная аттестация, в т.ч. с помощью платформ для онлайн-связи в период ДО.</p>

<p>В результате освоения дисциплины обучающийся должен <i>уметь</i>: классифицировать защищаемую информацию по видам тайны и степеням секретности; классифицировать основные угрозы безопасности информации;</p>	<p>Умения проводить классификацию информации по видам тайны и степени секретности, основных угроз информации в профессиональной деятельности</p>	<p>Оценка результатов выполнения практической работы Текущий и рубежный контроль, в т.ч.с применением ДОТ, выполнение контрольных заданий и итоговых тестов с применением ЭО. Промежуточная аттестация, в т.ч. с помощью платформ для онлайн-связи в период ДО.</p>
--	--	--

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ ПО ОСВОЕНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ ПРИ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОГО ОБУЧЕНИЯ И ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

Согласно ст. 16 Федерального закона под **электронным обучением** понимается организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников.

Под **дистанционными образовательными технологиями** понимаются образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

Электронное обучение предполагает использование информации, содержащейся в базах данных, и информационных технологий и информационно-телекоммуникационных сетей для ее обработки и передачи при взаимодействии обучающихся и педагогических работников. Дистанционные образовательные технологии реализуются через информационно-телекоммуникационные сети, когда обучающиеся и педагогические работники находятся на расстоянии.

То есть и в том, и в другом случае предусматривается использование компьютера и сетевой инфраструктуры, но при электронном обучении это инструменты непосредственного взаимодействия обучающихся и педагогических работников, а при дистанционных образовательных технологиях – удаленного.

ОСНОВНЫЕ ВИДЫ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ С ПРИМЕНЕНИЕМ ДОТ:

лекции, реализуемые во всех технологических средах: работа в аудитории с электронными учебными курсами под руководством методистов-организаторов, в сетевом компьютерном классе в системе on-line (система общения преподавателя и обучающихся в режиме реального времени) и системе off-line (система общения, при которой преподаватель и обучающиеся обмениваются информацией с временным промежутком) в форме теле- и видеолекций и лекций-презентаций;

практические, семинарские и лабораторные занятия во всех технологических средах: видеоконференции, собеседования в режиме chat (система общения, при которой участники, подключенные к Интернет, обсуждают заданную тему короткими текстовыми сообщениями в режиме реального времени),

занятия в учебно-тренировочных классах, компьютерный лабораторный практикум, профессиональные тренинги с использованием телекоммуникационных технологий;

учебная практика, реализация которой возможна посредством информационных технологий; индивидуальные и групповые консультации, реализуемые во всех технологических средах: электронная почта, chat-конференции, форумы, видеоконференции;

самостоятельная работа обучающихся, включающая изучение основных и дополнительных учебно-методических материалов; выполнение расчетно-практических и расчетно-графических, тестовых и иных заданий; выполнение курсовых проектов, написание

курсовых работ, тематических рефератов и эссе; работу с интерактивными учебниками и учебно-методическими материалами, в том числе с сетевыми или автономными мультимедийными электронными учебниками, практикумами; работу с базами данных удаленного доступа;

текущие и рубежные контроли, промежуточные аттестации с применением ДОТ.

ОСНОВНЫЕ ВИДЫ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ С ПРИМЕНЕНИЕМ ЭО:

самостоятельная интерактивная и контролируемая интенсивная работа студента с учебными материалами, включающими в себя видеолекции, слайды, методические рекомендации по изучению дисциплины и выполнению контрольных заданий, контрольные и итоговые тесты.