

**Департамент образования Ярославской области  
Государственное профессиональное образовательное учреждение  
Ярославской области  
Переславский колледж им. А. Невского**

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

**ОП.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**по специальности 10.02.05 Обеспечение информационной безопасности  
автоматизированных систем**

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Организация-разработчик: ГПОУ ЯО Переславский колледж им. А. Невского

Разработчик: Болдырев Е.П., преподаватель ГПОУ ЯО Переславский колледж им. А. Невского

**СОДЕРЖАНИЕ**

<b>1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ</b>	<b>4</b>
<b>2. СТРУКТУРА УЧЕБНОЙ ДИСЦИПЛИНЫ</b>	<b>5</b>
<b>3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ</b>	<b>9</b>
<b>4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ</b>	<b>11</b>

## 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

### 1.1. Место дисциплины в структуре рабочей основной профессиональной образовательной программы:

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.

### 1.2. Цель и планируемые результаты освоения дисциплины:

Код ПК, ОК	Умения	Знания
ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4	<ul style="list-style-type: none"> <li>– классифицировать защищаемую информацию по видам тайны и степеням секретности;</li> <li>– классифицировать основные угрозы безопасности информации;</li> </ul>	<ul style="list-style-type: none"> <li>– сущность и понятие информационной безопасности, характеристику ее составляющих;</li> <li>– место информационной безопасности в системе национальной безопасности страны;</li> <li>– виды, источники и носители защищаемой информации;</li> <li>– источники угроз безопасности информации и меры по их предотвращению;</li> <li>– факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;</li> <li>– жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;</li> <li>– современные средства и способы обеспечения информационной безопасности;</li> <li>– основные методики анализа угроз и рисков информационной безопасности;</li> </ul>

**2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ****2.1. Объем учебной дисциплины и виды учебной работы**

<b>Вид учебной работы</b>	<b>Объем в часах</b>
<b>Обязательная учебная нагрузка</b>	64
в том числе:	
теоретическое обучение	38
практические занятия (если предусмотрено)	24
<i>Самостоятельная работа</i>	-
<b>Промежуточная аттестация в форме дифференцированного зачета</b>	<b>2</b>

## 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	Осваиваемые элементы компетенций
1	2	3	4
<b>Раздел 1. Теоретические основы информационной безопасности</b>		<b>34</b>	
<b>Тема 1.1.</b> Основные понятия и задачи информационной безопасности	<b>Содержание учебного материала</b>	<b>6</b>	ОК 3, ОК 6, ОК 9, ПК.2.4
	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 неинформированности в области информационной безопасности.	2	
<b>Тема 1.2.</b> Основы защиты информации	<b>Содержание учебного материала</b>	<b>10</b>	ОК 3, ОК 6, ОК 9, ПК 2.4
	Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.	2	
	Понятия государственной тайны и конфиденциальной информации.	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 в основную деятельность организации. Понятие Политики безопасности.	2	
	<b>Практические занятия</b>	<b>6</b>	
	Определение объектов защиты на типовом объекте информатизации.	2	
	Классификация защищаемой информации по видам тайны и степеням	2	

	конфиденциальности.		
	Классификация защищаемой информации по степеням конфиденциальности.	2	
<b>Тема 1.3.</b> Угрозы безопасности защищаемой информации.	<b>Содержание учебного материала</b>	<b>6</b>	ОК 3, ОК 6, ОК 9, ПК.2.4
	Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации.	2	
	Каналы и методы несанкционированного доступа к информации	2	
	Уязвимости. Методы оценки уязвимости информации	2	
	<b>Практические занятия</b>	<b>6</b>	
	Определение угроз объекта информатизации.	2	
	Классификация угроз объекта информатизации.	2	
	Построение модели угроз безопасности информации	2	
<b>Раздел 2. Методология защиты информации</b>		<b>28</b>	
<b>Тема 2.1.</b> Методологические подходы к защите информации	<b>Содержание учебного материала</b>	<b>4</b>	ОК 3, ОК 6, ОК 9, ПК 2.4
	Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.	2	
	Виды мер и основные принципы защиты информации.	2	
<b>Тема 2.2.</b> Нормативно правовое регулирование защиты информации	<b>Содержание учебного материала</b>	<b>6</b>	ОК 3, ОК 6, ОК 9, ОК 10
	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	
	<b>Практические занятия</b>	<b>6</b>	
	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	2	
	Работа с документами системы сертификации РФ в области защиты информации	2	

	Работа с нормативно-методическими и руководящими документами	2	
Тема 2.3. Защита информации в автоматизированных (информационных) системах	<b>Содержание учебного материала</b>	<b>6</b>	ОК 3, ОК 6, ОК 9, ОК 10
	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	
	<b>Практические занятия</b>	<b>6</b>	
	Выбор мер защиты информации для автоматизированного рабочего места	2	
	Организационные меры защиты информации на предприятии	2	
	Политика информационной безопасности организации	2	
<b>Промежуточная аттестация по учебной дисциплине в форме дифференцированного зачета</b>		<b>2</b>	
<b>Всего</b>		<b>64</b>	

### 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Реализация программы дисциплины требует наличия учебного кабинета информационной безопасности, лаборатории информационных технологий.

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

##### 1.2.1. Основные печатные источники:

1. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. –М.: Академия. 2017.

##### 1.2.2. Дополнительные печатные источники:

1. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. – М.: Издательство КДУ.

2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: Учебн. пособие для вузов. - М: Горячая линия-Телеком, 2006. - 544 с.: ил. Допущено УМО ИБ.

3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита. Учебное пособие. – М.: Инфа-М. 2016.

4. Бабаш А.В. Информационная безопасность. Лабораторный практикум (+CD) : учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — 2-е изд., стер. – М. : КНОРУС, 2016.

5. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. Учебное пособие. – М.: МГТУ им. Баумана. 2016.

6. Нестеров С.А. Основы информационной безопасности. Учебное пособие. – С-Пб.: Лань. 2016.

7. Пржегорлинский В.Н. Организационно-правовое обеспечение информационной безопасности. –М.: Академия. 2015.

8. Проскурин В.Г. Защита программ и данных: Учебное пособие для ВУЗов. - – М.: Академия. 2012.

9. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. – С-Пб.: Изд. Питер. 2017.

10. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях. ДМК Пресс, 2012.

### **3.2.3 Периодические издания:**

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Журналы Защита информации. Инсайд: Информационно-методический журнал
3. Информационная безопасность регионов: Научно-практический журнал
4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: <http://cyberrus.com/>
5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: <http://bit.mephi.ru/>

### **1.2.3. Электронные источники:**

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) [www.fstec.ru](http://www.fstec.ru)
2. Информационно-справочная система по документам в области технической защиты информации [www.fstec.ru](http://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](http://www.consultant.ru)
5. Справочно-правовая система «Гарант» » [www.garant.ru](http://www.garant.ru)
6. Федеральный портал «Российское образование [www.edu.ru](http://www.edu.ru)
7. Федеральный правовой портал «Юридическая Россия» <http://www.law.edu.ru/>
8. Российский биометрический портал [www.biometrics.ru](http://www.biometrics.ru)
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» <http://www.ict.edu.ru>
10. Сайт Научной электронной библиотеки [www.elibrary.ru](http://www.elibrary.ru)

#### 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Формы и методы оценки
<p>Знания:</p> <ul style="list-style-type: none"> <li>– сущность и понятие информационной безопасности, характеристику ее составляющих;</li> <li>– место информационной безопасности в системе национальной безопасности страны;</li> <li>– виды, источники и носители защищаемой информации;</li> <li>– источники угроз безопасности информации и меры по их предотвращению;</li> <li>– факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;</li> <li>– жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;</li> <li>– современные средства и способы обеспечения информационной безопасности;</li> <li>– основные методики анализа угроз и рисков информационной безопасности.</li> </ul>	<p>Демонстрация знаний по курсу «Основы информационной безопасности» в повседневной и профессиональной деятельности.</p>	<p>Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий. Тестирование</p>

<p>Умения:</p> <ul style="list-style-type: none"><li>– классифицировать защищаемую информацию по видам тайны и степеням секретности;</li><li>– классифицировать основные угрозы безопасности информации;</li></ul>	<p>Умения проводить классификацию информации по видам тайны и степени секретности, основных угроз информации в профессиональной деятельности</p>	<p>Экспертное наблюдение в процессе практических занятий</p>
--	--	--