

**МИНОБРНАУКИ РОССИИ**  
**федеральное государственное бюджетное образовательное учреждение высшего образования**  
**«Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова»**  
**(БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова)**

УТВЕРЖДАЮ  
Декан факультета  
среднего профессионального  
образования

\_\_\_\_\_ Л.К. Шамина  
подпись

«09» февраля 2026 г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**  
**ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Для специальности  
среднего профессионального образования  
**09.02.11 РАЗРАБОТКА И УПРАВЛЕНИЕ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ**

Рабочая программа учебной дисциплины «Основы информационной безопасности» разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) среднего профессионального образования по специальности 09.02.11 РАЗРАБОТКА И УПРАВЛЕНИЕ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ.

Организация-разработчик:  
БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова

СОГЛАСОВАНО

Начальник отдела основных образовательных программ

\_\_\_\_\_/О.Ю. Иванова /

Председатель ПЦК «Информационные системы и программирование»

\_\_\_\_\_/А.С. Стукалова /

09 февраля 2026 г.

**Разработчики:**

\_\_\_\_\_/ А.С. Стукалова/

## **СОДЕРЖАНИЕ**

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ .....	4
2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	6
3 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ .....	10
4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	12

# **1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**

## **1.1 Область применения программы**

Рабочая программа учебной дисциплины «Основы информационной безопасности» является частью программы подготовки специалистов среднего звена (ППССЗ) по специальности СПО 09.02.11 Разработка и управление программным обеспечением.

Программа учебной дисциплины «Основы информационной безопасности» предназначена для формирования у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.

## **1.2 Место дисциплины в структуре основной профессиональной образовательной программы**

Учебная дисциплина «Основы информационной безопасности» является обязательной частью общепрофессионального цикла образовательной программы подготовки специалистов среднего звена по специальностям технического профиля на базе среднего общего образования. На изучение дисциплины отводится **72 часа**.

## **1.3 Цели и задачи дисциплины – требования к результатам освоения дисциплины**

Цель дисциплины «Основы информационной безопасности»: формирование у обучающихся понимания основ информационной безопасности, практических навыков организации работ по обеспечению информационной безопасности на предприятиях и организациях.

Задачи дисциплины:

- способствовать освоению терминологического и понятийного аппарата теории информационной безопасности;
- изучить российское и зарубежное законодательство, а также особенности стандартов и спецификаций в области информационной безопасности;
- способствовать формированию знаний о возможных информационных угрозах и возможных средств защиты от них;
- изучить методологию и основные методы защиты информации от базовых угроз;
- способствовать формированию навыков оценки защищенности объектов и эффективности систем обеспечения информационной безопасности.

В рамках программы учебной дисциплины обучающимися осваиваются умения, знания, навыки:

Код ОК, ПК	Умения	Знания
ОК.01	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составлять план действия; определять необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника) / –	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности

ОК.02	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; / –	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств.
ОК.09	понимать тексты на базовые профессиональные темы / –	законодательство в области информационной безопасности; отраслевые стандарты и системы профессиональных сертификаций;
ПК 1.5	защищать информацию в базе данных, шифровать данные и обеспечивать их конфиденциальность; классифицировать и выявлять основные угрозы безопасности; классифицировать защищаемую информацию по видам тайны и степеням секретности;	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 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.

#### 1.4. Количество часов на освоение учебной дисциплины

Объем учебной нагрузки обучающегося 72 часа, в том числе обязательной аудиторной учебной нагрузки обучающегося 40 часов, самостоятельной работы – 30 часов, промежуточной аттестации – 2 часа.

## **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>Объем образовательной нагрузки</b>	72
<b>Обязательная аудиторная учебная нагрузка</b>	40
в том числе:	
теоретическое обучение	20
практические занятия	20
<b>Самостоятельная работа</b>	30
<b>Консультация</b>	–
<b>Промежуточная аттестация</b>	2

## 2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала	Объем часов	Формируемые общие компетенции и профессиональные компетенции
<b>Раздел 1. Теоретические основы информационной безопасности</b>		<b>32</b>	
<b>Тема 1.1</b> Основные понятия и задачи информационной безопасности	<b>Содержание учебного материала</b>	<b>8</b>	ОК 01 ОК 02 ОК 09 ПК 1.5
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.	2	
	<b>В том числе практических занятий</b> Практическое занятие № 1. Определение объектов защиты на типовом объекте информатизации.	2	
	<b>Самостоятельная работа обучающихся</b> Работа с основными информационными источниками. Создание перечня защищаемых объектов и систем в рамках профессиональной деятельности.	4	
<b>Тема 1.2</b> Нормативно-правовое регулирование защиты информации	<b>Содержание учебного материала</b>	<b>10</b>	ОК 01 ОК 02 ОК 09 ПК 1.5
	Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)	4	
	<b>В том числе практических занятий</b> Практическое занятие № 2. Стандарты и спецификации в области информационной безопасности.	2	
	<b>Самостоятельная работа обучающихся</b> Сравнительный анализ Российского и зарубежного законодательства в области информационной безопасности.	4	
<b>Тема 1.3</b> Классификация безопасности и документооборот	<b>Содержание учебного материала</b>	<b>14</b>	ОК 01 ОК 02 ОК 09 ПК 1.5
	Основные понятия и механизмы информационной безопасности. Классы безопасности. Правила и порядок оформления документов	4	
	<b>В том числе практических занятий</b> Практическое занятие № 3. Документооборот, как способ защиты информации. Практическое занятие № 4. Классификация защищаемой информации по видам тайны и степеням конфиденциальности.	4	
	<b>Самостоятельная работа обучающихся</b> Порядок и оформление документов, документооборот по индивидуальному заданию.	6	
<b>Раздел 2 Методология защиты информации</b>		<b>36</b>	
<b>Тема 2.1</b> Угрозы безопасности защиты информации	<b>Содержание учебного материала</b>	<b>16</b>	
	Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Угрозы информационной безопасности. Способы защиты информации. Аппаратные и программные средства обеспечения безопасности государства.	4	ОК 01 ОК 02 ОК 09

Наименование разделов и тем	Содержание учебного материала	Объем часов	Формируемые общие компетенции и профессиональные компетенции
и основы защиты информации	<b>В том числе практических занятий</b> Практическое занятие № 4. Антивирусные программы и их использование. Резервное копирование и восстановление данных. Управление доступом к данным.	6	ПК 1.5
	<b>Самостоятельная работа обучающихся</b> Сравнительный анализ уязвимости программных продуктов.	6	
<b>Тема 2.2</b> Защита сетевой инфраструктуры	<b>Содержание учебного материала</b>	<b>10</b>	ОК 01 ОК 02 ОК 09 ПК 1.5
	Защита от информационных утечек. Технические каналы утечки информации, способы обнаружения и предупреждения утечки информации по техническим каналам связи. Защита информации, содержащей коммерческую, государственную и иные виды тайн. Комплексные средства защиты информации.	4	
	<b>В том числе практических занятий</b> Практическое занятие № 5. Использование VPN и межсетевых экранов.	2	
	<b>Самостоятельная работа обучающихся</b> Анализ типичных ошибок, влияющих на безопасность.	4	
<b>Тема 2.3</b> Методологические подходы к защите информации	<b>Содержание учебного материала</b>	<b>10</b>	ОК 01 ОК 02 ОК 09 ПК 1.5
	Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Инженерная защита и техническая охрана объектов информатизации	2	
	<b>В том числе практических занятий</b> Практическое занятие № 6. Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности.	2	
	<b>Самостоятельная работа обучающихся</b> Выбор мер защиты информации для автоматизированного рабочего места	6	
Защита проектов	Презентация и защита итогового проекта по выбранной тематике	2	
<b>Промежуточная аттестация</b>		2	
<b>Всего:</b>		<b>72</b>	



### **3 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ**

#### **3.1. Требования к минимальному материально-техническому обеспечению**

Реализация программы учебной дисциплины «Основы информационной безопасности» предполагает наличие специализированного учебного кабинета – компьютерного класса, в котором имеется возможность обеспечить свободный доступ в телекоммуникационную сеть «Интернет» во время учебного занятия и в период внеучебной деятельности обучающихся.

Оборудование учебного кабинета:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- учебно-планирующая документация;
- мультимедийное оборудование.

Технические средства обучения:

- компьютер с лицензионным программным обеспечением на рабочем месте преподавателя с выходом в Internet;
- мультимедийный проектор;
- мультимедийный экран или интерактивная доска;

#### **3.2. Информационное обеспечение реализации программы**

В процессе освоения программы дисциплины ОП.05 «Основы информационной безопасности» обучающимся предоставлена возможность доступа к электронным учебным материалам по дисциплине, имеющимся в свободном доступе в сети Интернет (электронным книгам, практикумам, тестам).

##### **3.2.1 Литература**

**Основная:**

1. Овчинникова, Е. А. Информационная безопасность. Организационноправовые основы. В 2 частях. Ч. 1: учебное пособие для СПО / Е. А. Овчинникова, Г. В. Попков. — Саратов: Профобразование, 2024. — 191 с. — ISBN 978-5-4488-1876-9 (ч. 1), 978-5-4488-1883-7. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROОбразование: [сайт]. — URL: <https://profspo.ru/books/139029>

2. Овчинникова, Е. А. Информационная безопасность. Организационноправовые основы. В 2 частях. Ч. 2: учебное пособие для СПО / Е. А. Овчинникова, Г. В. Попков. — Саратов: Профобразование, 2024. — 167 с. — ISBN 978-5-4488-1877-6 (ч. 2), 978-5-4488-1883-7. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROОбразование: [сайт]. — URL: <https://profspo.ru/books/139030>

1. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург: Лань, 2024. — 84 с. — ISBN 978-5-507-48808-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/394547>

2. Баланов, А. Н. Комплексная информационная безопасность: учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург: Лань, 2024. — 284 с. — ISBN 978-5-507-49251-0. — Текст: электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/414950>

**Дополнительная:**

1. Нестеров, С. А. Основы информационной безопасности: учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/195510>

2. Прохорова, О. В. Информационная безопасность и защита информации: учебник для спо / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург: Лань, 2024. — 124 с. — ISBN 978-5-507-47517-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/385082>

4. Моргунов, А. В. Информационная безопасность: учебнометодическое пособие / А. В. Моргунов. — Новосибирск: Новосибирский государственный технический университет, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROОбразование: [сайт]. — URL: <https://profspo.ru/books/98708>

5. Смышляев, А. Г. Информационная безопасность. Лабораторный практикум: учебное пособие / А. Г. Смышляев. — Белгород: Белгородский государственный технологический университет им. В.Г.

Шухова, ЭБС АСВ, 2015. — 102 с. — ISBN 2227-8397. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/66655>

6. Солонская, О. И. Средства защиты информации: учебное пособие для СПО / О. И. Солонская. — Саратов: Профобразование, 2022. — 88 с. — ISBN 978-5-4488-1504-1. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/125578>

**Интернет-ресурсы:**

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 ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины «Основы информационной безопасности» осуществляется преподавателем в процессе проведения самостоятельных работ, практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий.

<i>Результаты обучения</i>	<i>Критерии оценки</i>	<i>Методы оценки</i>
<p><b>Знать:</b></p> <p>методы планирования своей работы;</p> <ul style="list-style-type: none"> <li>- методы и приемы, используемые для недопущения / устранения угроз информационной безопасности;</li> <li>- методы и средства сбора информации и ее хранения;</li> <li>- средства управления, связанные с использованием, обработкой, хранением и передачей данных;</li> <li>- законодательство в области информационной безопасности;</li> <li>- отраслевые стандарты и системы профессиональных сертификаций;</li> </ul> <p>сущность и понятие информационной безопасности, характеристику ее составляющих;</p> <ul style="list-style-type: none"> <li>- место информационной безопасности в системе национальной безопасности страны;</li> <li>- виды, источники и носители защищаемой информации; 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; современные средства и способы обеспечения информационной безопасности;</li> <li>- основные методики анализа угроз и рисков информационной безопасности.</li> </ul>	<p>демонстрирует знания методов планирования своей работы;</p> <p>демонстрирует знание методов и приемов, используемых для недопущения / устранения угроз информационной безопасности;</p> <p>демонстрирует знание методов и средств сбора информации и ее хранения;</p> <p>владеет средствами управления, связанными с использованием, обработкой, хранением и передачей данных;</p> <p>демонстрирует знание законодательства в области информационной безопасности;</p> <p>демонстрирует знание отраслевых стандартов и систем профессиональных сертификаций;</p> <p>знает сущность и понятие информационной безопасности, характеристику ее составляющих;</p> <p>осознает место информационной безопасности в системе национальной безопасности страны;</p> <p>демонстрирует знание о видах, источниках и носителях защищаемой информации;</p> <p>источниках угроз безопасности информации и меры по их предотвращению;</p> <p>осведомлен о факторах, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;</p> <p>знает жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;</p> <p>современные средства и способы обеспечения информационной безопасности;</p> <p>знает основные методики анализа угроз и рисков информационной безопасности.</p>	<p>Тестирование.</p> <p>Устный опрос.</p> <p>Экспертное наблюдение выполнения практических работ и видов работ по практике.</p> <p>Промежуточная аттестация.</p>
<p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- применять аналитические навыки для диагностики и устранения неисправностей в работе информационных систем и сетей;</li> <li>- точно описывать угрозу и документировать решение проблемы;</li> <li>- выбирать меры защиты информации для автоматизированного рабочего места;</li> <li>- осуществлять поиск информации в открытых источниках и работать с технической документацией;</li> <li>- читать или разрабатывать документацию к существующей или проектируемой информационной структуре предприятия</li> <li>- классифицировать основные угрозы безопасности информации;</li> <li>- классифицировать защищаемую</li> </ul>	<p>демонстрирует аналитические навыки для диагностики и устранения неисправностей в работе информационных систем и сетей;</p> <p>демонстрирует умение описывать угрозу и документировать решение проблемы;</p> <p>выбирает эффективные меры защиты информации для автоматизированного рабочего места;</p> <p>эффективно осуществляет поиск информации в открытых источниках и работать с технической документацией;</p> <p>демонстрирует навыки чтения и разработки документации к существующей или проектируемой информационной структуре предприятия</p> <p>верно классифицирует основные угрозы безопасности информации;</p>	<p>Тестирование.</p> <p>Устный опрос.</p> <p>Наблюдение за ходом выполнения практических работ.</p> <p>Промежуточная аттестация.</p>

информацию по видам тайны и степеням секретности; - выявлять информационные угрозы; - анализировать и разрабатывать процедуры интеграции, тестирования, эксплуатации, сопровождения механизмов информационной безопасности.	демонстрирует умение классификации защищаемой информации по видам тайны и степеням секретности; демонстрирует навыки выявления информационных угроз; демонстрирует навыки анализа и разработки процедур интеграции, тестирования, эксплуатации, сопровождения механизмов информационной безопасности.	
---	---	--

Форма итогового контроля по учебной дисциплине «Основы информационной безопасности»  
— зачет.