

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ЧИТИНСКИЙ ИНСТИТУТ
КОЛЛЕДЖ



УТВЕРЖДАЮ:
Первый заместитель директора
Н.В. Расвский
«31» мая 2023 г.

Рабочая программа учебной дисциплины

Информационная безопасность

Специальность: 09.02.07 Информационные системы и программирование
Квалификация Программист

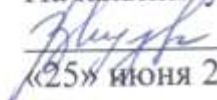
Чита
2023

Рабочая программа по дисциплине ОПЦ.15 «Информационная безопасность» разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования 09.02.07 Информационные системы и программирование.

Актуализировано 25 июня 2024 г.

Согласовано:

Начальник учебной части колледжа

 В.С. Кузнецова

«25» июня 2024 г.

Принята на заседании методической комиссии

Протокол № 10 от «25» июня 2024 г.

Председатель методической комиссии:

 Т.В. Порядина

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	стр. 4
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	6
3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ	12
4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ	15

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 09.02.07 Информационные системы и программирование, квалификация специалист по тестированию в области информационных технологий.

Программа учебной дисциплины может быть использована в профессиональной подготовке, а также при разработке программ дополнительного профессионального образования специалистов технического профиля.

1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина «Информационная безопасность» принадлежит к вариативной части общепрофессионального цикла.

Дисциплина «Информационная безопасность» является общепрофессиональной, устанавливающей базовые знания для усвоения профессиональных компетенций.

1.3. Цели и задачи учебной дисциплины — требования к результатам освоения учебной дисциплины:

Целью преподавания дисциплины «Информационная безопасность» является изучение комплекса проблем информационной безопасности организаций различных типов и направлений деятельности; построения, функционирования и совершенствования правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации; изучение понятий и видов защищаемой информации по законодательству РФ. Изучение данной дисциплины подготавливает студентов к освоению специальных программных средств, связанных с их будущей деятельностью.

Задачи изучения дисциплины включают:

- овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности;
- освоение системных комплексных методов защиты информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения;
- ознакомление с современными законодательными и нормативно-правовыми проблемами обеспечения информационной безопасности;
- приобретение теоретических и практических навыков по основам использования современных методов правовой защиты государственной, коммерческой, служебной, профессиональной и личной тайны, персональных

данных в компьютерных системах;

- лицензирования и сертификации в области защиты информации;
- формирование практических навыков и способностей осуществления мероприятий по обеспечению защиты информации с помощью программно-аппаратных средств.

В результате изучения обязательной части учебного цикла обучающийся по общепрофессиональным дисциплинам должен иметь **практический опыт в:**

- обеспечении защиты программного обеспечения компьютерных систем программными средствами;

уметь:

- использовать методы защиты программного обеспечения компьютерных систем;

- анализировать риски и характеристики качества программного обеспечения;

- выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами.

знать:

- основные средства и методы защиты компьютерных систем программными и аппаратными средствами.

Изучение дисциплины способствует освоению **общей компетенции:**

ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

Изучение дисциплины способствует освоению **профессиональной компетенции**, соответствующих основному виду профессиональной деятельности: сопровождение и обслуживание программного обеспечения компьютерных систем:

ПК 4.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.

1.4. Количество часов на освоение программы учебной дисциплины:

Максимальная учебная нагрузка обучающегося – **90 часов**, в том числе:

- обязательная аудиторная учебная нагрузка обучающегося – **76 часов**;

- самостоятельная работа обучающегося – **14 часов**.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	90
Обязательная аудиторная учебная нагрузка (всего)	76
в том числе:	
Лекционные занятия	38
Практические занятия	38
Самостоятельная работа обучающегося (всего)	14
в том числе:	
внеаудиторная самостоятельная работа	0
в том числе:	
отчеты по выполненным лабораторным работам	14
<i>Итоговая аттестация в форме зачета</i>	

2.2. Тематический план и содержание учебной дисциплины Информационная безопасность

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень Освоения
1	2	3	4
Тема 1. Основы информационной безопасности	Содержание: 1. Понятие информационной безопасности. Актуальность информационной безопасности. Принципы обеспечения информационной безопасности. Структура информационной безопасности. 2. Система защиты информации. Структура системы защиты информации РФ. Угрозы безопасности в информационной сфере. Комплексный подход к защите информации.	4	ОК 01, ПК 4.4
	Практические занятия: 1. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы № 1 «Защита информации в файлах данных средствами MS Office». 2. Защита отчета по лабораторной работе № 1. Ответы на контрольные вопросы.		
	Самостоятельная работа обучающихся: изучение теоретического материала для подготовки к выполнению лабораторной работы и ответов на контрольные вопросы, выполнение отчета.	1	
Тема 2. Правовая защита информации	Содержание: 1. Структура нормативной базы Российской Федерации по вопросам информационной безопасности. Правовая защита интересов личности, общества и государства от информационных угроз. 2. Защита информации по режиму доступа. Классификация информации по видам тайны и степеням конфиденциальности. Защита государственной тайны. Защита коммерческой тайны. Защита персональных данных.	4	ОК 01, ПК 4.4
	Практические занятия: 1. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы №2 «Создание резервной копии средствами ОС Windows». 2. Защита отчета по лабораторной работе № 2. Ответы на контрольные вопросы.		
	Самостоятельная работа обучающихся: изучение теоретического материала для подготовки к выполнению лабораторной работы и ответов на контрольные вопросы, выполнение отчета.	1	
Тема 3.	Содержание:	4	ОК 01,

Организационная защита информации	1. Зоны ответственности. Локальные нормативные акты в области информационной безопасности. Административный уровень организационной защиты информации. Оценка рисков		ПК 4.4
--	--	--	--------

	<p>информационной безопасности. Политика информационной безопасности.</p> <p>2. Процедурный уровень организационной защиты информации. Организация службы безопасности предприятия. Организация конфиденциального документооборота. Грифы ограничения доступа к документам.</p> <p>Практические занятия:</p> <p>1. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы №3 «Стойкость парольной защиты».</p> <p>2. Защита отчета по лабораторной работе № 3. Ответы на контрольные вопросы.</p> <p>Самостоятельная работа обучающихся: изучение теоретического материала для подготовки к выполнению лабораторной работы и ответов на контрольные вопросы, выполнение отчета.</p>		
		4	
		1	
Тема 4. Защита информации в компьютерных системах	Содержание:	8	ОК 01, ПК 4.4
	1. Анализ угроз информационной безопасности компьютерных систем. Технологии защиты информации в компьютерных системах.		
	2. Идентификация, аутентификация и управление доступом. Обеспечение безопасности операционных систем.		
	3. Безопасность межсетевых обмена данными. Технологии межсетевых экранов.		
	4. Анализ защищенности и обнаружение атак. Технологии резервного копирования и восстановления данных.		
	Практические занятия:	8	
1. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы №4 «Средства обеспечения безопасности ОС Windows».			
2. Защита отчета по лабораторной работе № 4. Ответы на контрольные вопросы.			
3. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы №5 «Шифрованная файловая система MS Windows».			
4. Защита отчета по лабораторной работе № 5. Ответы на контрольные вопросы.			
Самостоятельная работа обучающихся: изучение теоретического материала для подготовки к выполнению лабораторной работы и ответов на контрольные вопросы, выполнение отчета.	1		
Тема 5. Методы криптографического преобразования информации	Содержание:	4	ОК 01, ПК 4.4
	1. Классификация методов криптографического закрытия информации. Симметричные криптосистемы. Криптосистемы с открытым ключом.		
	2. Практическое применение криптографии. Квантовая криптография. Стеганография. Электронная подпись.		

	<p>Практические занятия:</p> <p>1. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы № 6 «Элементы криптоанализа».</p> <p>2. Защита отчета по лабораторной работе № 6. Ответы на контрольные вопросы.</p>	4	
	<p>Самостоятельная работа обучающихся: изучение теоретического материала для подготовки к выполнению лабораторной работы и ответов на контрольные вопросы.</p>	1	
Тема 6. Вредоносное программное обеспечение	<p>Содержание:</p> <p>1. Условия существования вредоносных программ. Классификация вредоносных программ. Эволюция компьютерных вирусов.</p> <p>2. Защита компьютерных систем от воздействия вредоносных программ. Основы работы антивирусных программ. Защита от СПАМА.</p>	4	ОК 01, ПК 4.4
	<p>Практические занятия:</p> <p>1. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы № 7 «Применение электронной подписи».</p> <p>2. Защита отчета по лабораторной работе № 7. Ответы на контрольные вопросы.</p>	4	
	<p>Самостоятельная работа обучающихся: изучение теоретического материала для подготовки к выполнению лабораторной работы и ответов на контрольные вопросы, выполнение отчета.</p>	1	
Тема 7. Инженерно-техническая защита информации	<p>Содержание:</p> <p>1. Технические каналы утечки информации. Средства выявления каналов утечки информации.</p> <p>2. Методы и способы защиты информации от утечки по техническим каналам.</p> <p>3. Физическая укрепленность объекта информатизации.</p>	6	ОК 01, ПК 4.4
	<p>Практические занятия:</p> <p>1. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы № 8 «Удаление и восстановление компьютерной информации».</p> <p>2. Защита отчета по лабораторной работе № 8. Ответы на контрольные вопросы.</p>	4	
	<p>Самостоятельная работа обучающихся: изучение теоретического материала для подготовки к выполнению лабораторной работы и ответов на контрольные вопросы.</p>	1	
Тема 8. Управление информационной безопасностью	<p>Содержание:</p> <p>1. Ответственность, за правонарушения в области информационной безопасности. Лицензирование, сертификация и аттестация в сфере защиты информации. Комплексный подход к защите информации.</p> <p>2. Стандарты и спецификации в области информационной безопасности. Анализ защищенно</p>	4	ОК 01, ПК 4.4

	сти информационной системы. Управление информационной безопасностью. Практические правила управления информационной безопасностью.		
	Практические занятия:	6	
	1. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы № 9 «Анализ защищенности веб-приложений».		
	2. Защита отчета по лабораторной работе № 9. Ответы на контрольные вопросы.		
	3. Итоговый тест.		
	Самостоятельная работа обучающихся: изучение теоретического материала для подготовки к выполнению лабораторной работы и ответов на контрольные вопросы, выполнение отчета.	1	
	Всего:	76	

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

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

Лаборатория «Программного обеспечения и сопровождения компьютерных систем» оснащенная необходимым для реализации программы учебной дисциплины оборудованием:

- автоматизированные рабочие места на 12-15 обучающихся (процессор не ниже Core i3, оперативная память объемом не менее 4 Гб) или аналоги;
- автоматизированное рабочее место преподавателя (процессор не ниже Core i3, оперативная память объемом не менее 4 Гб) или аналоги;
- проектор и экран;
- маркерная доска;

Программное обеспечение общего и профессионального назначения

3.2. Информационное обеспечение обучения

Основная литература:

1. Овчинникова, Е. А. Информационная безопасность: учебное пособие для СПО / Е. А. Овчинникова. — Саратов: Профобразование, 2024. — 166 с. — ISBN 978-5-4488-1872-1. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/139028> — Режим доступа: для авторизир. пользователей

2. Самойлова, Е. М. Информационная безопасность: учебное пособие для СПО / Е. М. Самойлова, М. В. Виноградов. — Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2023. — 135 с. — ISBN 978-5-4488-1662-8, 978-5-4497-2244-7. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/131646> — Режим доступа: для авторизир. пользователей.

3. Фомин, Д. В. Информационная безопасность: учебное пособие для СПО / Д. В. Фомин. — Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2022. — 218 с. — ISBN 978-5-4488-1351-1, 978-5-4497-1565-4. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/118458> — Режим доступа: для авторизир. пользователей.

4. Суворова, Г. М. Основы информационной безопасности: учебное пособие для СПО / Г. М. Суворова. — Саратов: Профобразование, 2021. — 214 с. — ISBN 978-5-4488-1294-1. — Текст: электронный // Электронный ресурс

цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/108005> — Режим доступа: для авторизир. пользователей.

Дополнительная литература:

1. Овчинникова, Е. А. Информационная безопасность. Организационно-правовые 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 PROФобразование: [сайт]. — URL: <https://profspo.ru/books/139029> — Режим доступа: для авторизир. пользователей

2. Овчинникова, Е. А. Информационная безопасность. Организационно-правовые 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 PROФобразование: [сайт]. — URL: <https://profspo.ru/books/139030> — Режим доступа: для авторизир. пользователей

3. Сафонова, Л. А. Экономические аспекты информационной безопасности: учебное пособие для СПО / Л. А. Сафонова. — Саратов: Профобразование, 2024. — 116 с. — ISBN 978-5-4488-1878-3. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/139055> — Режим доступа: для авторизир. пользователей

4. Технологии защиты информации в компьютерных сетях: учебное пособие для СПО / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суоров. — 2-е изд. — Саратов: Профобразование, 2024. — 368 с. — ISBN 978-5-4488-1014-5. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/139767> — Режим доступа: для авторизир. пользователей

5. Суорова, Г. М. Основы информационной безопасности: учебное пособие для СПО / Г. М. Суорова. — Саратов: Профобразование, 2021. — 214 с. — ISBN 978-5-4488-1294-1. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/108005> — Режим доступа: для авторизир. пользователей

6. Ревнивых, А. В. Информационная безопасность в организациях: учебное пособие / А. В. Ревнивых. — Москва: Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст: электронный // Электронный ресурс

цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/108227> — Режим доступа: для авторизир. пользователей.

7. Куликов, С. С. Информационная безопасность глобальных компьютерных сетей: практикум / С. С. Куликов. — Воронеж: Воронежский государственный технический университет, ЭБС АСВ, 2021. — 66 с. — ISBN 978-5-7731-0970-9. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/118613> — Режим доступа: для авторизир. пользователей.

8. Куликов, С. С. Информационная безопасность локальных компьютерных сетей: практикум / С. С. Куликов. — Воронеж: Воронежский государственный технический университет, ЭБС АСВ, 2021. — 57 с. — ISBN 978-5-7731-0969-3. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/118614> — Режим доступа: для авторизир. пользователей.

9. Галатенко, В. А. Основы информационной безопасности: учебное пособие / В. А. Галатенко. — 3-е изд. — Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/97562> — Режим доступа: для авторизир. пользователей.

10. Брюхомицкий, Ю. А. Безопасность информационных технологий. В 2 частях. Ч.1: учебное пособие / Ю. А. Брюхомицкий. — Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2020. — 171 с. — ISBN 978-5-9275-3571-2 (ч.1), 978-5-9275-3526-2. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование: [сайт]. — URL: <https://profspo.ru/books/107943> — Режим доступа: для авторизир. пользователей.

Интернет-ресурсы:

1. <http://window.edu.ru/> — Единое окно доступа к образовательным ресурсам.

2. <http://citforum.ru/> — Сервер Информационных Технологий.

3. <http://fcior.edu.ru/> — Федеральный центр электронных образовательных ресурсов.

4. <http://www.intuit.ru/> — Национальный Открытый Университет.

5. <http://www.ixbt.com> — специализированный российский информационно-аналитический сайт с самыми актуальными новостями из сферы IT.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляются преподавателем в процессе выполнения лабораторных работ, тестирования, а также ответов на контрольные вопросы.

<i>Результаты обучения</i>	<i>Критерии оценки</i>	<i>Формы и методы оценки</i>
<p><i>Перечень знаний, осваиваемых в рамках дисциплины:</i></p> <ul style="list-style-type: none"> - Основные средства и методы защиты компьютерных систем программными и аппаратными средствами. 	<p>«Отлично» — теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко.</p>	<p>Текущий контроль в форме:</p> <ul style="list-style-type: none"> - наблюдения за выполнением практического задания. <p>(деятельностью студента);</p>
<p><i>Перечень умений, осваиваемых в рамках дисциплины:</i></p> <ul style="list-style-type: none"> - Использовать методы защиты программного обеспечения компьютерных систем. - Анализировать риски и характеристики качества программного обеспечения. - Выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами. 	<p>«Хорошо» — теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками.</p> <p>«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.</p> <p>«Неудовлетворительно» — теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.</p>	<ul style="list-style-type: none"> - защиты отчетов по лабораторным работам; - оценки выполнения практического задания (работы); - устных опросов; - компьютерного тестирования на знание терминологии по теме. <p>Зачет по дисциплине.</p>