ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ

**«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ГУМАНИТАРНО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»**

КАЛМЫЦКИЙ ФИЛИАЛ

УТВЕРЖДАЮ
И.о. директора филиала
_____ Пашнанов Э.Л.
«23» 04 2020 г.

РАБОЧАЯ ПРОГРАММА

УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.17. Информационная безопасность

по специальности

09.02.03 Программирование в компьютерных системах

квалификация – техник-программист

Элиста, 2020 г.

ОДОБРЕНА
Предметно-цикловой комиссией
естественнонаучных и
математических дисциплин

протокол № 7
от « 22 » 04 2020 г.

председатель предметно-цикловой комиссии
Катрикова Ц.Ю. _____

Разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02. 03 Программирование в компьютерных системах

заместитель директора по учебно-методической работе
Новгородова В.В. _____

составитель:
_____ Хамуров С.Б., высшая квалификационная категория, преподаватель Калмыцкого филиала ФГБОУИ ВО «Московский гуманитарно экономический университет»

рецензенты:
_____ Пипенко В.В., первая квалификационная категория, преподаватель Калмыцкого филиала ФГБОУИ ВО «Московский гуманитарно экономический университет»

_____ Агеев С.С., заместитель начальника отдела обеспечения деятельности, противодействия коррупции кадров и защиты информации, Министерства финансов Республики Калмыкия

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью образовательной программы в соответствии с ФГОС по специальности СПО 09.02.03 Программирование в компьютерных системах

1.2. Место учебной дисциплины в структуре образовательной программы.

Учебная дисциплина «Информационная безопасность» относится к общепрофессиональным дисциплинам профессионального цикла вариативной части циклов ППССЗ, направлена на формирование общих и профессиональных компетенций:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ПК 1.6. Разрабатывать компоненты проектной и технической документации с использованием графических языков спецификаций.

ПК 2.4. Реализовывать методы и технологии защиты информации в базах данных.

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

В результате освоения учебной дисциплины обучающийся должен уметь:

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- применять основные правила и документы системы сертификации Российской Федерации;

- классифицировать основные угрозы безопасности информации.

В результате освоения учебной дисциплины обучающийся должен знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- источники угроз информационной безопасности и меры по их предотвращению;
- жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности.

1.4. Использование часов вариативной части ППССЗ

№	Дополнительные знания, умения	№, наименование темы	Количество часов	Обоснование включения в рабочую программу
1.	Умения: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; применять основные правила и документы системы сертификации Российской Федерации; классифицировать основные угрозы безопасности информации. Знания: сущность и понятие информационной безопасности, характеристику ее составляющих; место информационной безопасности в системе национальной безопасности страны; источники угроз информационной безопасности и меры по их предотвращению; жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи; современные средства и способы обеспечения ин-	Все	76	запрос работодателя на дополнительные результаты освоения ППССЗ

	формационной безопасности.			

1.5. Рекомендуемое количество часов на освоение программы учебной дисциплины:

максимальной учебной нагрузки обучающегося 114 часов, в том числе: обязательной аудиторной учебной нагрузки обучающегося 76 часов; самостоятельной работы обучающегося 38 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Количество часов
Максимальная учебная нагрузка (всего)	114
Обязательная аудиторная учебная нагрузка (всего)	76
в том числе:	
практические занятия	24
Самостоятельная работа обучающегося (всего)	38
в том числе:	
Знакомство с учебной литературой. Выполнение домашней работы Написание рефератов Работа с информационными ресурсами Интернета Самостоятельная работа с книгой Решение профессиональных задач	
Промежуточная аттестация в форме дифференцированного зачета	

2.2. Тематический план содержание учебной дисциплины «Информационная безопасность»

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся		Объем часов	Уровень усвоения
1	2		3	4
	7 семестр		60/40	
Раздел I. Теоретические основы информационной безопасности			30/20	
Тема 1.1. Основные задачи и функции в сфере обеспечения информационной безопасности.	Содержание учебной дисциплины		6/4	
	1	Понятие информация и информационная безопасность. Объекты информационной безопасности. Задачи в сфере информационной безопасности.	2	1
	2	Защита человека от опасной информации. Основные функции государственной системы по обеспечению информационной безопасности.	2	2
	Самостоятельная работа обучающихся: Самостоятельная работа с книгой. Выполнение домашней работы		2	
Тема 1.2. Отечественный и зарубежные стандарты в области информационной безопасности.	Содержание учебной дисциплины		9/6	
	1	Аспекты информационной безопасности. Стандарты безопасности РФ, Европы и других стран.	2	1
	2	Цели и задачи защиты информации.	2	2
	3	Основные элементы политики безопасности	2	2
	Самостоятельная работа обучающихся: Знакомство с учебной литературой. Выполнение домашней работы		3	
Тема 1.3. Защита информации	Содержание учебной дисциплины		3/2	
	1	Безопасная, надежная системы защиты. Основные угрозы информационной безопасности.	2	1
	Самостоятельная работа с книгой. Выполнение домашней работы		1	
Тема 1.4. Основные предметные направления защиты информа-	Содержание учебной дисциплины		3/2	
	1	Понятие об основных предметных направлениях защиты информации: государ-	2	1

ции		ственная, коммерческая, банковская, профессиональная, служебная тайна. Особенности правоотношений в этой области.		
	Самостоятельная работа обучающихся: Самостоятельная работа с книгой. Выполнение домашней работы		1	
Тема 1.5. Охрана персональных данных и интеллектуальной собственности	Содержание учебной дисциплины		3/2	
	1	Персональные данные как объект защиты. Охрана интеллектуальной собственности.	2	1
	Самостоятельная работа обучающихся: Самостоятельная работа с книгой. Выполнение домашней работы		1	
Тема 1.6.Правовые основы защиты информации	Содержание учебной дисциплины		3/2	
	1	Ознакомление с правовой базой защиты информации.	2	1
	Самостоятельная работа с книгой. Выполнение домашней работы		1	
Тема 1.7. Ответственность за нарушение законодательства в информационной сфере.	Содержание учебной дисциплины		3/2	
	1	Административная и уголовная ответственность за нарушение законодательства в информационной сфере.	2	1
	Самостоятельная работа обучающихся: Самостоятельная работа с книгой. Выполнение домашней работы		1	
Раздел II. Защита информации в Автоматизированных системах обработки данных (АСОД)			36/24	
Тема 2.1. Предмет и объекты защиты информации в АСОД	Содержание учебной дисциплины		3/2	
	1	Надежность информации в АСОД, системная защита. Жизненный цикл информации в АСОД . Виды информации в АСОД подлежащие защите	2	1
	Самостоятельная работа с книгой. Выполнение домашней работы		1	
Тема 2.2. Дестабилизирующие факторы АСОД	Содержание учебной дисциплины		3/2	
	1	Факторы влияющие на уязвимость информации в АСОД	2	1
	Самостоятельная работа с книгой. Выполнение домашней работы		1	
Тема 2.3. Причины нарушения целостности информации	Содержание учебной дисциплины		3/2	
	1	Группы причин нарушения целостности элементов АСОД. Каналы НСД	2	1
	Самостоятельная работа с книгой. Выполнение домашней работы		1	
Тема 2.4. Причины случайных воздействий	Содержание учебной дисциплины		3/2	
	1	Выявления причин случайных воздействий на АСОД	2	1
	Самостоятельная работа с книгой. Выполнение домашней работы		1	

Тема 2.5. Преднамеренные угрозы безопасности АСОД	Содержание учебной дисциплины		3/2	
	1	Возможные причины преднамеренных воздействий на АСОД. Мотивация нарушителей.	2	1
	Самостоятельная работа с книгой. Выполнение домашней работы		1	
Тема 2.6. Механизмы защиты	Содержание учебной дисциплины		3/2	
	Практическое занятие			
	1	Ознакомление с возможными механизмами защиты.	2	
	Самостоятельная работа с книгой. Выполнение домашней работы.		1	
Тема 2.7. Методы и системы защиты информации	Содержание учебной дисциплины		3/2	
	1	Основные принципы и понятия касающиеся методов и систем защиты информации	2	1
	Самостоятельная работа с книгой. Выполнение домашней работы		1	
Тема 2.8. Аппаратно - программные средства защиты	Содержание учебной дисциплины		3/2	
	1	Рассмотрение групп входящих в состав аппаратно-программных средств защиты	2	1
	Самостоятельная работа с книгой. Выполнение домашней работы		1	
Тема 2.9. Системы идентификации и аутентификации.	Содержание учебной дисциплины		6/4	
	Практические занятия		4	
	1	Системы распознавания	2	
	2	Системы установления подлинности	2	
	Самостоятельная работа с книгой. Выполнение домашней работы		2	
	8 семестр		54/36	
Тема 2.10. Использование простого и динамического пароля	Содержание учебной дисциплины		3/2	
	Практическое занятие		2	
	1	Отличие применения простого и динамического пароля	2	
	Самостоятельная работа обучающихся: Самостоятельная работа с книгой. Выполнение домашней работы.		1	
Тема 2.11. Общие сведения о контроле информационной целостности	Содержание учебной дисциплины		3/2	
	1	Общие сведения о контроле информационной целостности. Способы определения модификаций информации. Организация контроля.	2	1
	Самостоятельная работа обучающихся: Самостоятельная работа с книгой. Выполнение		1	

	домашней работы			
Раздел III. Общие сведения о криптографических методах защиты.			12	
Тема 3.1. Криптология и основные этапы ее развития.	Содержание учебной дисциплины		6/4	
	1	Основные этапы развития криптологии.	2	1
	2	До научные методы шифрования.	2	2
	Самостоятельная работа обучающихся: Самостоятельная работа с книгой. Выполнение домашней работы		2	
Тема 3.2. Методы криптографического преобразования данных.	Содержание учебной дисциплины		9/6	
	Практические занятия		6	
	1	Основные понятия и определения. Классификация методов	2	
	2	Простая подстановка	2	
	3	Реализация метода шифрования Цезаря на компьютере.	2	
	Самостоятельная работа обучающихся: Самостоятельная работа обучающихся: Самостоятельная работа с книгой. Выполнение домашней работы		3	
Тема 3.3. Характеристики криптографических средств защиты.	Содержание учебной дисциплины		3/2	
	1	Стойкость и трудоемкость методов закрытия информации.	2	1
	Самостоятельная работа обучающихся: Самостоятельная работа с книгой. Выполнение домашней работы		1	
Раздел IV. Защита информации в ПК			30/20	
Тема 4.1. Особенности защиты информации в персональном компьютере (ПК).	Содержание учебной дисциплины		3/2	
	1	Отличие персональных компьютеров от других систем цифровых вычислительных машин.	2	1
	Самостоятельная работа обучающихся: Самостоятельная работа с книгой. Выполнение домашней работы		1	
Тема 4.2. Угрозы информации в персональных компьютерах.	Содержание учебной дисциплины		6/4	
	1	Особенности архитектурного построения персональных компьютеров, ее основные каналы коммуникации.	2	1
	2	Методы противодействия угрозам данных в персональном компьютере.	2	1
	Самостоятельная работа с книгой. Выполнение домашней работы		1	
Тема 4.3. Цели и функции защи-	Содержание учебной дисциплины		3/2	

ты информации в персональных компьютерах.	1	Обеспечение целостности информации, предупреждение модификации и т.п.	2	1
	Самостоятельная работа обучающихся: Самостоятельная работа с книгой. Выполнение домашней работы		1	
Тема 4.4. Защита персональных компьютеров от несанкционированного доступа.	Содержание учебной дисциплины		15/10	
	Практические занятия		10	
	1	Основные механизмы защиты	2	
	2	Аутентификация реализованная на персональным компьютере.	2	
	3	Разграничение доступа к элементам защищаемой информации	2	
	4	Объективные условия которые повышают угрозы несанкционированного доступа.	2	
	5	Аутентификация. Алгоритмы аутентификации.	2	
	Самостоятельная работа обучающихся: Самостоятельная работа с книгой. Выполнение домашней работы		5	
Раздел V. Компьютерные вирусы и антивирусные программы.				
Тема 5.1. Классификация вирусов.	Содержание учебной дисциплины		3/2	
	1	Классификация по среде обитания, способу заражения, деструктивным возможностям Алгоритм функционирования некоторых вирусов Методы профилактики и защиты от вирусов. Антивирусные программы.	2	1
	Самостоятельная работа обучающихся: Самостоятельная работа с книгой. Выполнение домашней работы		1	
	Всего		114/76	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1. — ознакомительный (узнавание ранее изученных объектов, свойств);
2. — репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. — продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия лаборатории Информационно-коммуникационных систем, мастерских «Корпоративная защита от внутренних угроз информационной безопасности», «Анализ защищённости информационных систем от внешних угроз».

Оборудование лаборатории:

- рабочие места студентов, оборудованные персональными компьютерами (Proceccor: Intel Core i5, частота не менее 2,4 ГГц, поддержка памяти DDR4 до 128 ГБ, ОЗУ DIMM, DDR4 не менее 8 Гб; HDD не менее 500 Гб; SSD не менее 400Гб);
- лабораторные учебные макеты;
- рабочее место преподавателя (Proceccor: Intel Core i5, частота не менее 2,4 ГГц, поддержка памяти DDR4 до 128 ГБ, ОЗУ DIMM, DDR4 не менее 8 Гб; HDD не менее 500 Гб; SSD не менее 400Гб);
- учебно-методическое обеспечение модуля;
- интерактивная доска, комплект презентаций;
- антивирусные программные комплексы;
- программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности (ПО для защиты от утечек типа InfoWatch Traffic Monitor 6.9 или аналог, InfoWatch Device Monitor 6.9 или аналог, InfoWatch Crawler 1.4 или аналог, соответствующие лицензии на весь период проведения , БД PostgreSQL 9.5 (под Windows) или функциональный аналог);
- программные и программно-аппаратные средства обнаружения атак (вторжений), поиска уязвимостей (Защита конечных точек Secret Net Studio, Соболь, Terminal, Защита сети АПКШ «Континент», Сервер доступа «Континент» и СКЗИ «Континент-АП»);
- средства уничтожения остаточной информации в запоминающих устройствах;
- программные средства криптографической защиты информации (Крипто-Про).

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, дополнительной литературы, интернет – ресурсов.

Основные источники:

1. Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. Криптографическая защита информации в объектах информационной инфраструктуры: учебник для студ. учреждений сред. проф. образования - издательский центр «Академия», 2020 г. – 288 с.
2. Васильков А.В., Васильков А.А. Информационные системы и их безопасность: учеб. пособие/ А.В.Васильков, А.А.Васильков.-М.: ФОРУМ,2012.-528 с.-(Профессиональное образование).
3. Партыка Т.Л., Попов И.И.Информационная безопасность. Учебное пособие для студ. учреждений сред.проф. образования.-2-е изд., испр. и доп.-М.:ФОРУМ: ИНФРА-М,2007.-368с.- (Профессиональное образование)
4. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие.-М.: ИД «ФОРУМ»: ИНФРА-М,2012.- 416с.- (Профессиональное образование).

Дополнительные источники:

1. Основы информационной безопасности : опорный конспект / Е.А. Рыбакова. - СПб.: Изд-во СЗТУ, 2016. - 49 с.
2. Калмыков И.А. Криптографические методы защиты информации [Электронный ресурс]: лабораторный практикум/ Калмыков И.А., Науменко Д.О., Гиш Т.А.— Электрон. Текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2015.— 109 c

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения различных форм учебных занятий.

Результаты обучения (освоенные умения, усвоенные знания)	Коды формируемых профессиональных и общих компетенций	Формы и методы контроля и оценки результатов обучения
1	2	3
Умения:	ОК 1-5,8,9 ПК 1.6, 2.4	
-классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; -применять основные правила и документы системы сертификации Российской Федерации; -классифицировать основные угрозы безопасности информации;		Интерпретация результатов наблюдений за деятельностью обучающихся в процессе освоения образовательной программы Текущий и рубежный контроль в форме: - устного опроса - тестирования - практических занятий - самостоятельных работ по темам дисциплины.
Знания:		
-сущность и понятие информационной безопасности, характеристику ее составляющих; -место информационной безопасности в системе национальной безопасности страны; -источники угроз информационной безопасности и меры по их предотвращению; -жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи; -современные средства и способы обеспечения информационной безопасности		

Приложение

ВОПРОСЫ К ДИФФЕРЕНЦИРОВАННОМУ ЗАЧЕТУ

1. Дайте характеристику составляющих "информационной безопасности" применительно к вычислительным сетям.
2. Перечислите основные механизмы безопасности.
3. Укажите какие механизмы безопасности используются для обеспечения конфиденциальности трафика.
4. Какие виды избыточности могут использоваться в вычислительных сетях.
5. Как обнаружить загрузочный вирус.
6. Какие характерные черты макровируса.
7. Является ли наличие скрытых листов в Excel признаком заражения макровирусом.
8. Перечислите наиболее распространенные пути заражения компьютеров вирусами.
9. Как ограничить заражение макровирусом при работе с офисными приложениями.
10. Как обнаружить резидентный вирус.
11. Как проверить систему на наличие макровируса.
12. Перечислите основные этапы алгоритма обнаружения вируса.
13. Какие особенности заражения вирусами при использовании электронной почты.
14. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
15. Как ограничить заражение макровирусом при работе с офисными приложениями.
16. Как рассматривается сеть в концепции протокола IP.
17. Как классифицируются удаленные угрозы "по характеру воздействия".
18. Охарактеризуйте удаленные угрозы "по цели воздействия".
19. Как классифицируются удаленные угрозы "по расположению субъекта и объекта угрозы".
20. Может ли пассивная угроза привести к нарушению целостности информации.
21. Что такое подсеть и сегмент сети и чем они отличаются.
22. Перечислите основные причины успешной реализации удаленных угроз информационной безопасности в вычислительных сетях.
23. Почему виртуальное соединение не обеспечивает требуемого уровня защиты вычислительных сетей.
24. В чем заключаются преимущества сети с выделенными каналами.
25. Какой из алгоритмов поиска более безопасный.

26. Что является следствием недостаточной аутентификации субъектов и объектов вычислительных сетей.
27. Может ли быть нарушена целостность информации при отсутствии в распределенных вычислительных сетях возможности контроля за маршрутом сообщений.
28. Как повысить защищенность вычислительных сетей при установлении виртуального соединения.
29. Перечислите угрозы нарушения конфиденциальности, особенности и примеры реализации угрозы.
30. Перечислите основные угрозы нарушения целостности данных, особенности и примеры реализации угрозы.
31. Понятие политики безопасности информационных систем. Назначение политики безопасности.
32. Перечислите требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
33. Опишите Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
34. Раскройте функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
35. Перечислите основные Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
36. Раскройте Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
37. Что такое Идентификация и аутентификация при входе в информационную систему, использование парольных схем, недостатки парольных схем.
38. Что такое Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
39. Опишите Биометрические средства идентификации и аутентификации пользователей.
40. Раскройте Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
41. Раскройте суть методов несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.
42. Какое место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.

43. Какие средства обеспечения информационной безопасности в ОС Windows 8, 10. Разграничение доступа к данным. Групповая политика.
44. Как файловая система NTFS обеспечивает информационную безопасность в Windows 7/8/10. Списки контроля доступа к данным (ACL) их роль в разграничении доступа к данным.
45. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
46. Какие причины нарушения безопасности информации при ее обработке криптографическими средствами.
47. Какие существуют каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
48. Какие физические средства обеспечения информационной безопасности.
49. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
50. Какие программно-аппаратные средства защиты информационных ресурсов применяются в Интернете. Межсетевые экраны, их функции и назначения.

РЕЦЕНЗИЯ

на рабочую программу по дисциплине ОП.17. Информационная безопасность для специальности СПО 09.02.03 Программирование в компьютерных системах, разработанную преподавателем Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет» Хамуровым С.Б.

Представленная рабочая программа учебной дисциплины «Информационная безопасность» разработана в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.03 Программирование в компьютерных системах.

Структура рабочей программы соответствует структуре примерных программ учебных дисциплин среднего профессионального образования.

Рецензируемая рабочая программа учебной дисциплины имеет чёткую структуру и включает все необходимые компоненты.

В паспорте рабочей программы определена область применения программы, отражено место учебной дисциплины в структуре образовательной программы, раскрываются цели, задачи дисциплины - требования к результатам освоения учебной дисциплины.

Объем учебной дисциплины, виды учебной работы, тематический план и содержание учебной дисциплины раскрывают структуру и содержание учебной дисциплины. Указанные объем часов максимальной, обязательной аудиторной учебной нагрузки, практических занятий, самостоятельной работы обучающихся и форма промежуточной аттестации соответствуют учебному плану. Виды самостоятельной работы позволяют привить обучающимся умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечить высокий уровень успеваемости в период обучения. В тематическом плане и содержании учебной дисциплины раскрывается последовательность изучения разделов и тем программы, показываются распределение учебных часов по разделам, темам и указывается уровень освоения. Дидактические единицы, отраженные в содержании учебного материала, направлены на качественное усвоение учебного материала. Для приобретения практических навыков и повышения уровня знаний предусмотрены практические занятия.

Условия реализации учебной дисциплины определяют требования к необходимому материально-техническому обеспечению к оборудованию учебного кабинета и техническим средствам обучения. Информационное обеспечение обучения содержит современный перечень рекомендуемых учебных изданий, дополнительной литературы и интернет-ресурсов.

Контроль и оценка результатов освоения учебной дисциплины содержит результаты обучения, формы и методы контроля и оценки результатов обучения, которые осуществляются преподавателем в процессе проведения различных форм учебных занятий.

Рецензируемая рабочая программа рекомендуется для реализации в образовательном процессе.

Рецензент Пипенко В.В., преподаватель Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно- экономический университет»

РЕЦЕНЗИЯ

на рабочую программу по дисциплине ОП.17. Информационная безопасность для специальности СПО 09.02.03 Программирование в компьютерных системах, разработанную преподавателем Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет» Хамуровым С.Б.

Представленная рабочая программа учебной дисциплины «Информационная безопасность» разработана с учетом требований Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.03 Программирование в компьютерных системах.

Структура рабочей программы соответствует структуре примерных программ учебных дисциплин среднего профессионального образования на основе Федеральных государственных образовательных стандартов СПО.

В паспорте рабочей программы определена область применения программы, место учебной дисциплины в структуре образовательной программы, сформулированы цели и задачи, требования к результатам освоения учебной дисциплины.

Объем учебной дисциплины и виды учебной работы, предусмотренные структурой учебной дисциплины, соответствуют тематическому содержанию учебной дисциплины.

Содержание программы направлено на приобретение обучающимися знаний, умений, направленных на формирование общих и профессиональных компетенций, определенных ФГОС СПО по специальности 09.02.03 Программирование в компьютерных системах и соответствует объему часов, указанному в рабочем учебном плане.

Материально-техническое обеспечение включает наличие учебного кабинета, оснащенного оборудованием и техническими средствами обучения.

Информационное обеспечение обучения содержит перечень современных учебных изданий, дополнительной литературы и интернет-ресурсов.

Контроль и оценка результатов освоения учебной дисциплины содержит умения, знания, профессиональные, общие и профессиональные компетенции, формы, методы контроля оценки результатов обучения и осуществляется преподавателем в процессе проведения различных форм учебных занятий.

Рабочая программа позволит студентам в достаточной мере освоить учебную дисциплину, овладеть общими и профессиональными компетенциями, необходимых для качественного освоения программы подготовки специалистов среднего звена.

Рабочая программа дисциплины «Информационная безопасность» рекомендуется к применению в учебном процессе Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет».

Рецензент _____ Агеев С.С., заместитель начальника отдела обеспечения деятельности, противодействия коррупции кадров и защиты информации, Министерства финансов Республики Калмыкия