УТВЕРЖДАЮ

И.О. директора филиала
_____ А.В. Смехова
30.06.2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

СМК-РПД-8.3-7/3/4-24.39-2017

ОП.15 Методы и средства защиты информации

(наименование дисциплины)

Трудоёмкость в часах: **60**

Образовательная программа **09.02.04** Информационные системы (по отраслям)

(шифр и наименование специальности)

Разработана в соответствии с учебным планом направления подготовки (специальности) **09.02.04** Информационные системы (по отраслям)

(шифр по ОКСО и наименование)

Учебный план утвержден ректором университета, 20.06.2017 г.

Рабочая программа обсуждена на заседании цикловой методической комиссии (ЦМК)

протокол от 26.06.2017 г. №10

Председатель ЦМК _____ О.М. Жаткина

(подпись)

Разработал(и) Рабцун Е.С., преподаватель

Находка

Рабочая программа учебной дисциплины «Методы и средства защиты информации» реализуется за счет часов вариатива. Дисциплина включена в образовательную программу для реализации дополнительных знаний и умений в области защиты информации в соответствии с требованиями работодателей.

Год начала подготовки ООП 2017 г.

Организация-разработчик: Находкинский филиал Федерального государственного бюджетного образовательного учреждения высшего образования «Морской государственный университет имени адмирала Г.И. Невельского».

Рецензенты: Степанова Юлия Викторовна, начальник отдела информационных систем регионального центра «Дальний Восток» ООО «ЕВРАЗТехника»

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ…… 4

2. СТРУКТУРА СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ…… 7

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ……..…… 13

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ…….. 15

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ…… 17

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.15 Методы и средства защиты информации

1.1. Область применения рабочей программы

Программа учебной дисциплины «Методы и средства защиты информации» является вариативной частью основной образовательной программы среднего профессионального образования по подготовке специалистов среднего звена в соответствии с ФГОС по специальности 09.02.04 Информационные системы (по отраслям). Содержание программы составлено в соответствии с производственными потребностями и отраслевой направленности, согласовано на цикловой методической комиссии.

1.2. Место учебной дисциплины в структуре основной образовательной программы (ППССЗ):

П.00 Профессиональный цикл, в раздел ОП.00 Общепрофессиональные дисциплины

1.3 Цели и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины

В результате освоения учебной дисциплины студент должен **уметь:**

- применять методы защиты информации в АИС;
- обеспечить разноуровневый доступ к информационным ресурсам АИС;
- реализовать политику безопасности в АИС;
- обеспечить антивирусную защиту информации;
- 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 студент 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.

Дисциплина способствует формированию:

- общих 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 6 Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7 Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

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.

- профессиональных компетенций:

ПК 1.1. Собирать данные для анализа использования и функционирования информационной системы, участвовать в составлении отчетной документации, принимать участие в разработке проектной документации на модификацию информационной системы.

ПК 1.5. Разрабатывать фрагменты документации по эксплуатации информационной системы.

ПК 1.6. Участвовать в оценке качества и экономической эффективности информационной системы.

ПК 1.7. Производить инсталляцию и настройку информационной системы в рамках своей компетенции, документировать результаты работ.

ПК 1.9. Выполнять регламенты по обновлению, техническому сопровождению и восстановлению данных информационной системы, работать с технической документацией.

ПК 1.10. Обеспечивать организацию доступа пользователей информационной системы в рамках своей компетенции.

ПК 2.6. Использовать критерии оценки качества и надежности функционирования информационной системы.

1.4 Количество часов на освоение рабочей программы учебной дисциплины

максимальной учебной нагрузки обучающегося 60 часов, в том числе: обязательной аудиторной учебной нагрузки обучающегося 40 часов; самостоятельной работы обучающегося 20 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)	*60*
Обязательная аудиторная учебная нагрузка (всего)	*40*
в том числе:	
лабораторные работы	*-*
практические занятия	*20*
контрольные работы	
Самостоятельная работа обучающегося (всего)	*20*
в том числе:	
Реферирование подготовка конспекта подготовка сообщений подготовка презентаций	
Итоговая аттестация в форме ***контрольной работы***	

2.2.Тематический план и содержание учебной дисциплины

ОП.15 «Методы и средства защиты компьютерной информации»

Наименование разделов и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся		Объем часов	Уровень освоения
1	2		3	4
Введение		*Содержание учебного материала*	**1**	1
	1	Значимость информации в современном мире. Актуальность проблемы информационной безопасности. Предмет, задачи курса «Методы и средства защиты компьютерной информации». Роль и значение курса в подготовке специалистов по защите информации. Место курса среди других дисциплин учебного плана.	1	
Тема 1. Основные понятия и определения предмета защиты информации	*Содержание учебного материала*		**9**	
	1	Понятие информации, *защиты информации,* информационной системы, безопасности автоматизированных систем обработки информации. Цель защиты информации. Базовые свойства информации: конфиденциальность, целостность, доступность.	1	2
	2	Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя. Причины несанкционированного доступа к информации. Последствия несанкционированного доступа к информации.	1	
	3	Понятие угрозы, классификация угроз. Понятие уязвимости, атаки на компьютерную систему. Понятие риска. Задача специалиста по информационной безопасности.	1	
	4	Виды утечки информации. Понятие канала утечки информации, основные каналы утечки информации. Классификация злоумышленников.	1	
	5	Правовые (законодательные), морально-этические, организационно-административные, физические, аппаратно-программные меры обеспечения безопасности компьютерных систем.	1	
	Самостоятельная работа обучающихся		*4*	
		Систематическая проработка конспектов лекций, учебной литературы (по контрольным вопросам, составленным преподавателем, по вопросам к параграфам глав учебных пособий). Самостоятельное решение студентами поставленных задач, представленных в методических указаниях для выполнения самостоятельной работы. Форма контроля: проверка записей студентов, опрос студентов по заданной теме, тестирование.		

Тема 2. Идентификация и аутентификация субъектов	*Содержание учебного материала*		**9**	
	1	Понятие идентификации, идентификатора, авторизации, аутентификации. Определение и назначение подсистемы идентификации и аутентификации. Стойкость ко взлому подсистемы идентификации и аутентификации. Классификация подсистем идентификации и аутентификации.	1	2
	2	Особенности парольных систем, основные типы угроз безопасности парольных систем. Требования к выбору и использованию паролей.	1	
	3	Понятие и примеры биометрических характеристик человека, особенность применения биометрических систем идентификации и аутентификации личности по сравнению с другими классами систем идентификации и аутентификации, коэффициент ошибочных отказов и ошибочных подтверждений, архитектура биометрических систем аутентификации, обучение биометрических систем.	1	
	Практические занятия			
	1	Количественная оценка стойкости парольной защиты	2	
	2	Биометрическая аутентификация пользователя по клавиатурному подчерку	2	
	Самостоятельная работа обучающихся		*2*	
	1	Систематическая проработка конспектов лекций, учебной литературы (по контрольным вопросам, составленным преподавателем, по вопросам к параграфам глав учебных пособий). Самостоятельное решение студентами поставленных задач, представленных в методических указаниях для выполнения самостоятельной работы. Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя, оформление отчетов и подготовка к их защите. Форма контроля: проверка записей студентов, опрос студентов по заданной теме, тестирование.		
Тема 3. Разграничение доступа к ресурсам	*Содержание учебного материала*		**6**	
	1	Принципы организации разноуровневого доступа в автоматизированных информационных системах. Понятие политики безопасности, цель создания политик безопасности. Классификация политик безопасности.	2	2
	Практические занятия			
	1	Реализация политик информационной безопасности	2	
	Самостоятельная работа обучающихся		2	
		Систематическая проработка конспектов лекций, учебной литературы (по контрольным вопросам, составленным преподавателем, по вопросам к параграфам глав учебных пособий). Самостоятельное решение студентами поставленных задач, представленных в методических указаниях для выполнения самостоятельной работы. Форма контроля: проверка записей студентов, опрос студентов по заданной теме, тестирование.		

Тема 4. Методы и средства криптографической защиты	*Содержание учебного материала*		**17**	
	1	Сравнимость по модулю m, полный набор вычетов по модулю m. Основные свойства сравнений. Простые и составные числа, свойства простых чисел. Задача факторизации чисел. Наибольший общий делитель. Числовые функции, имеющие большое значение в теории чисел и в криптографии.	1	2
	2	Понятие криптографии, шифрования и дешифрования, ключа шифровании, шифротекста, криптоалгоритма. Принципы функционирования криптографической системы. Классификация криптосистем.	1	
	3	Понятие криптоанализа, криптоаналитической атаки. Основные типы криптоаналитических атак, криптостойкость шифра. Требования к шифрам, используемым для криптографической защиты информации.	1	
	4	Принцип функционирования симметричных криптосистем. Шифрование методами перестановки. Шифрование методом замены. Суть метода. Шифры моноалфавитной (метод Цезаря, простая моноалфавитная замена, шифрующие таблицы Трисемуса) и многоалфавитной (шифр Гронсфельда)	1	
	Практические занятия			
	1	Методы криптографической защиты информации. Простейшие алгоритмы шифрования	2	
	2	Шифр многоалфавитной замены — шифрование методом Вернама.	1	
	3	Шифрование текстовой информации	2	
	4	Зашифровать и расшифровать выданное преподавателем сообщение с помощью алгоритма шифрования RSA.	1	
	5	Методы и алгоритмы стеганографического сокрытия данных	2	
	Самостоятельная работа обучающихся		*5*	
		Систематическая проработка конспектов лекций, учебной литературы (по контрольным вопросам, составленным преподавателем, по вопросам к параграфам глав учебных пособий). Самостоятельное решение студентами поставленных задач, представленных в методических указаниях для выполнения самостоятельной работы. Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя, оформление отчетов и подготовка к их защите. Подготовка к практическим занятиям с использованием методических рекомендаций преподавателя, оформление практических занятий. Форма контроля: проверка записей студентов, опрос студентов по заданной теме, тестирование.		
Тема 5. Контроль целостности информации	*Содержание учебного материала*		**4**	
	1	Электронный документооборот: преимущества и недостатки, проблемы, связанные с обеспечением целостности передаваемого документа и аутентификации подлинности его автора, возможности	1	2

		злоумышленника при реализации угроз, направленных на нарушение целостности передаваемых сообщений и подлинность их авторства, метод решения данных проблем.		
	2	Понятие электронно-цифровой подписи (ЭЦП), Процедура установки ЭЦП (подписывание документа), процедура проверки ЭЦП (аутентификация документа). Схема установки ЭЦП, схема проверки ЭЦП.	1	
	Самостоятельная работа обучающихся		*2*	
		Систематическая проработка конспектов лекций, учебной литературы (по контрольным вопросам, составленным преподавателем, по вопросам к параграфам глав учебных пособий). Самостоятельное решение студентами поставленных задач, представленных в методических указаниях для выполнения самостоятельной работы. Форма контроля: проверка записей студентов, опрос студентов по заданной теме, тестирование.		
Тема 6. Защита от разрушающих программных воздействий	*Содержание учебного материала*		**4**	
	1	Понятие опосредованного несанкционированного доступа, программы с потенциально опасными последствиями. Функции, свойственные таким программам, классы данных программ. Понятие и виды активизирующих событий. Модели взаимодействия прикладной программы и программы с потенциально опасными последствиями.	1	2
	2	Свойства вирусов, фазы исполнения вируса, основные подходы к классификации компьютерных вирусов. Средства борьбы с компьютерными вирусами. Признаки заражения, виды проявлений компьютерных вирусов. Способы обнаружения заражения.	1	
	Самостоятельная работа обучающихся		*2*	
		Систематическая проработка конспектов лекций, учебной литературы (по контрольным вопросам, составленным преподавателем, по вопросам к параграфам глав учебных пособий). Самостоятельное решение студентами поставленных задач, представленных в методических указаниях для выполнения самостоятельной работы. Форма контроля: проверка записей студентов, опрос студентов по заданной теме, тестирование.		
Тема 7. Исследование стандартных защитных средств ОС Windows и пакета MicrosoftOffice	*Содержание учебного материала*		**10**	
	1	Защита документов Microsoft Office. Управление подсистемой аудита в ОС Windows. Управление пользователями и их правами доступа в ОС Windows	-	
	Практические занятия			2
	1	Защита документов Microsoft Office	2	
		Управление подсистемой аудита в ОС Windows	2	
		Управление пользователями и их правами доступа в ОС Windows	2	
	Самостоятельная работа обучающихся		*3*	

		Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя, оформление отчетов и подготовка к их защите. Форма контроля: проверка отчетов, опрос студентов по заданной теме, тестирование.		
		Контрольная работа	1	
		Всего:	**60**	

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 РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Требования к минимальному материально-техническому обеспечению

Реализация рабочей программы учебной дисциплины осуществляется в учебном кабинете «Программирование и базы данных» и лаборатории «Информационные системы».

Оборудование учебного кабинета:

Методическое обеспечение:

- методические и справочные материалы;
- наглядные пособия;
- специализированное программное обеспечение.

Перечень основного оборудования:

- сетевой компьютерный класс с выходом в Интернет;
- комплекты «столы–стулья» (2 к 1) в количестве не менее 15 шт.;
- шкафы для методической литературы;
- огнетушитель;

Технические средства обучения:

- проектор;
- компьютерное рабочее место для преподавателя;
- принтер;
- сканер.

Компьютерное рабочее место преподавателя:

- процессор типа Pentium®;
- процессор с тактовой частотой не менее 2,66 ГГц
- ОЗУ не менее 512 Мб;
- HDD не менее 80 Гб;
- акустическая система.

Компьютерное рабочее место ученика:

- процессор с тактовой частотой не менее 2,66 ГГц;
- ОЗУ не менее 512 Мб;
- HDD не менее 80 Гб;
- компьютерные наушники и микрофон.

Программное обеспечение:

- операционная система;
- антивирусная программа;
- программа-архиватор;
- офисное ПО: текстовый процессор, табличный процессор, программа для создания мультимедийных презентаций;
- система управления базами данных;
- система программирования;
- система визуального проектирования.

3.2 Информационное обеспечение обучения. Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Литература:

1. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами В УП (2012) /ЭУ[1]
2. Емельянова Н. З., Партыка Т. Л., Попов И. И. Защита информации в персональном компьютере .(2009)f /ЭУ
3. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях (2012) /ЭУ
4. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства.(2010) /ЭУ

Интернет-ресурсы:

1. www.fstec.ru Федеральная служба по техническому и экспортному контролю
2. www.securitylab.ru Новости, статьи, обзоры уязвимостей и мнения аналитиков.
3. www.azi.ru Межрегиональная общественная организация «Ассоциация защиты информации»
4. www.infotecs.ru Производитель программных и программно-аппаратных VPN-решений и средств криптографической защиты информации.
5. www.infosec.ru Компания оказания услуг по обеспечению информационной безопасности автоматизированных систем различного назначения и любого уровня сложности.
6. www.infoforum.ru Инфофорум направлен на создание условий для взаимодействия специалистов в области обеспечения информационной безопасности в Российской Федерации
7. www.cnews.ru издание о высоких технологиях
8. www.coresecurity.com Сайт о защите информации

[1] ЭУ – электронный учебник

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий. Оценка качества освоения учебной программы включает текущий контроль успеваемости, промежуточную аттестацию по итогам освоения дисциплины. Текущий контроль проводится в форме устного опроса, компьютерного тестирования. Промежуточная аттестация по учебной дисциплине проводится в форме зачета.

Результаты обучения (освоенные умения, усвоенные знания)	**Коды формируемых профессиональных и общих компетенций**	**Формы и методы контроля и оценки результатов обучения**
В результате освоения учебной дисциплины обучающийся должен уметь: – применять методы защиты информации в АИС; – обеспечить разноуровневый доступ к информационным ресурсам АИС; – реализовать политику безопасности в АИС; – обеспечить антивирусную защиту информации; – 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 студент 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;	ОК1 ОК2 ОК5 ОК6 ОК7 ОК8 ОК4 ОК3 ОК9 ПК1.1 ПК1.5 ПК1.6 ПК1.7 ПК1.9 ПК1.10 ПК2.6 ОК1 ОК2 ОК5 ОК6 ОК7 ОК8 ОК4 ОК3 ОК9 ПК1.1 ПК1.5 ПК1.6 ПК1.7 ПК1.9 ПК1.10 ПК2.6	Контроль усвоения знаний проводится в форме тестирования и контрольных работ. Контроль формирования умений производится в форме защиты практических работ. Итоговая аттестация по дисциплине проходит в соответствии с учебным планом по специальности Критерием оценки результатов освоения дисциплины является способность выполнения конкретных профессиональных задач в ходе самостоятельного выполнения работ, решения проблемных задач; выполнения работ по образцу, инструкции или под руководством; узнавание ранее изученных объектов, свойств.

– жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи; – современные средства и способы обеспечения информационной безопасности.		

5 ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Использование образовательных технологий обеспечивает ориентирование студента в потоке информации, связанной с различными подходами к определению сущности, содержания, методов, форм развития и саморазвития личности; самоопределение в выборе оптимального пути и способов личностно-профессионального развития; систематизацию знаний, полученных студентами в процессе аудиторной работы. Практические занятия обеспечивают развитие и закрепление умений и навыков определения целей и задач саморазвития, а также принятия наиболее эффективных решений по их реализации.

При проведении занятий используются следующие технологии обучения.

Традиционные технологии обучения предполагают передачу информации в готовом виде, формируют учебные умения по образцу: репродуктивной, развивающей технологий, технологии системы консультант.

Активные технологии обучения предполагают организацию обучения как продуктивную творческую деятельность в режиме активного взаимодействия студентов с преподавателем: технология сотрудничества (коллективное и индивидуальное взаимодействие), дифференцированное обучение, личностно-ориентированное обучение.

Интерактивные технологии обучения предполагают организацию обучения как продуктивную творческую деятельность в режиме активного взаимодействия студентов друг с другом и с преподавателем: проблемно-развивающие технологии, технологии критического мышления, медиа технологии, информационно-компьютерные технологии.

Количество аудиторных часов согласно учебному плану по дисциплине - 80, в том числе проводимых в активной и интерактивной форме – 11 часов.

Активные и интерактивные формы проведения занятий

Раздел, тема	Виды учебной деятельности	Формы проведения занятий	Количество часов
Тема 1. Основные понятия и определения предмета защиты информации	*Теоретические занятия* Понятие информации, *защиты информации,* информационной системы, безопасности автоматизированных систем обработки информации	Дискуссия	1
	Виды утечки информации. Понятие канала утечки информации, основные каналы утечки информации. Классификация злоумышленников.	Урок-презентация	1
	Правовые (законодательные), морально-этические, организационно-административные, физические, аппаратно-программные меры обеспечения безопасности компьютерных систем.	Круглый стол	1

Тема 2. **Идентификация и аутентификация субъектов**	*Теоретическое занятие* Понятие идентификации, идентификатора, авторизации, аутентификации *Практическое занятие* Количественная оценка стойкости парольной защиты.	Дискуссия Работа в парах	1 2
Тема 4. **Методы и средства криптографической защиты**	*Теоретические занятия* Понятие криптографии, шифрования и дешифрования, ключа шифровании, шифротекста, криптоалгоритма Принцип функционирования симметричных криптосистем. Шифрование методами перестановки. Шифрование методом замены. Шифрование методом гаммирования.	Урок-презентация Работа в парах	1 1
Тема 5. **Контроль целостности информации**	*Теоретическое занятие* Электронный документооборот: преимущества и недостатки, проблемы, связанные с обеспечением целостности передаваемого документа	Дискуссия	1
Тема 7. **Исследование стандартных защитных средств ОС Windows и пакета MicrosoftOffice**	*Практическое занятие* Защита документов Microsoft Office	Мастер класс	2
			11

Использование активных и интерактивных образовательных технологий способствует активизации мыслительной деятельности и творческого потенциала студентов, повышению интереса и мотивации обучающихся, делает более эффективным усвоение материала, позволяет индивидуализировать обучение и ввести экстренную коррекцию знаний. Данные технологии обеспечивают формирование общих и профессиональных компетенций через осмысленное переживание индивидуальной и коллективной деятельности, формируют познавательную потребность и необходимость дальнейшего самообразования.

Разработчик:
Преподаватель Находкинский филиал
МГУ им.адм.Г.И.Невельского _____ Е.С. Рабцун

Дополнения и изменения в рабочей программе

на 20___/20____ учебный год

В рабочую программу вносятся следующие изменения:

Рабочая программа пересмотрена на заседании цикловой методической комиссии (ЦМК) _____

протокол от _____20___ г. № ____

Председатель ЦМК _____ / _____