МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САХАЛИНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для студентов по выполнению
практических занятий
по дисциплине

ОП.15. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

09.00.00 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

по специальности

09.02.03 Программирование в компьютерных системах

(базовый уровень подготовки)

Квалификация: техник-программист
Форма обучения: очная

Южно-Сахалинск
2014

УТВЕРЖДАЮ
Зам. директора по УР
__________ И.М. Ким
«25» сентября 2014 г.

Разработчик(и):
Агаширинова В.Ю., преподаватель
(указать Ф.И.О., должность)

Одобрено на заседании ПЦК
информационных
дисциплин
Протокол № 1 от «23» сентября 2014 г.
Председатель ПЦК
__________ Савешова О.Б.

Согласовано __________ Порфирова *зав.отделением* Порфирова Т.Б. информатики
подпись *Ф.И.О.*

СОДЕРЖАНИЕ

Пояснительная записка

1.1. Программа учебной дисциплины по выбору является частью основной профессиональной образовательной программы по специальностям СПО 230115 «Программирование в компьютерных системах».

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

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

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

- ✓ отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
- ✓ применять действующую законодательную базу в области информационной безопасности;
- ✓ разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.

В результате освоения учебной дисциплины обучающийся должен **знать:**

- ✓ содержание основных понятий обеспечения информационной безопасности;
- ✓ источники угроз безопасности информации;
- ✓ методы оценки уязвимости информации;
- ✓ методы создания, организации и обеспечения функционирования систем комплексной защиты информации;
- ✓ методы пресечения разглашения конфиденциальной информации;
- ✓ виды и признаки компьютерных преступлений

Программа учебной дисциплины предполагает освоение следующих общих компетенций (ОК):

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

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

ОК-3. Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.

ОК-4. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.

ОК-5. Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.

ОК-6. Работать в коллективе и команде, обеспечивать ее сплочение,

эффективно общаться с коллегами, руководством, потребителями.
ОК-7. Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.
ОК-8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознано планировать повышение квалификации.
ОК-9. Быть готовым к смене технологий в профессиональной деятельности.

В результате освоения учебной дисциплины, обучающиеся должны развивать профессиональные компетенции (ПК) в соответствии с основными видами профессиональной деятельности:

ПК-1.1. Выполнять разработку спецификаций отдельных компонент.
ПК-1.2. Осуществлять разработку кода программного продукта на основе готовых спецификаций на уровне модуля.
ПК-2.4. Реализовывать методы и технологии защиты информации в базах данных.

Методические рекомендации включают в себя:

1. Перечень тем и заданий для практических работ.
2. Методические указания и пояснения по выполнению данных работ.
3. Критерии оценки практических работ.
4. Формы контроля за выполнением данных работ.
5. Литературу, необходимую для выполнения данных работ.

Таблица № 1

Перечень тем и заданий для практических работ

№ работы	Название темы	Задание для практической работы	Кол-во часов
1.	Физические и организационные угрозы. Виды мер обеспечения информационной безопасности защита от несанкционированного доступа	Пр1 Анализ терминов и определений информационной безопасности. Госты и руководящие документы.	2
2.	Основные принципы построения систем защиты информации.	Пр2 Угрозы информации. Проведение анализа информации на предмет целостности	2
3.	Модели и основные принципы защиты информации Основы защиты конфиденциальной информации	Пр3 Определение коэффициентов важности, полноты, адекватности информации	2
4.		Пр4Методы обеспечения информационной безопасности РФ: правовые, организационно-технические, экономические.	2
5.	Алгоритмы шифрования	Пр5Классификация автоматизированных систем обработки информации по классу защиты информации	2
6.		Пр6 Уровни обеспечения безопасности. Основные составляющие информационной безопасности. Угрозы информационной безопасности. Основные задачи обеспечения информационной безопасности	2
7.	Алгоритмы шифрования – замена, подстановка, перестановка..	Пр7 Методы организационной защиты информации. Соотношение организационных методов с правовыми и техническими методами защиты информации при использовании технических средств передачи, обработки и хранения информации	2
8.		Пр8 Оценка безопасности информации на объектах ее обработки	2
9.		Пр9 Оценка безопасности информации на объектах ее обработки	2
10.		Пр10 «Анализ рисков информационной безопасности»	2
11.		Пр11 электронная цифровая подпись: понятие и структура. Понятие электронного сертификата. Модели систем сертификации.	2
12.		Пр12 Признаки появления вирусов. Методы защиты. Антивирусное программное обеспечение	2
13.		Пр13 «процедура аутентификации пользователя на основе пароля»	2
14.		Пр14 «программная реализация криптографических алгоритмов» Алгоритм шифрования – алгоритм хофмана	2
15.		Пр15 «программная реализация криптографических алгоритмов» Алгоритмы шифрования – замена, перестановка.	2
16.		Пр16 «программная реализация криптографических алгоритмов» Алгоритмы шифрования –подстановка.	2
17.		Пр17 «программная реализация криптографических алгоритмов» Алгоритмы шифрования – алгоритм вижинера	2
18.	Защита от утечки информации по техническим каналам	Пр18 «Механизмы контроля целостности данных»	2
19.		Пр19 «Алгоритмы поведения вирусных и других вредоносных программ»	2

20.		Пр20 «Алгоритмы предупреждения и обнаружения вирусных угроз»	2
21.	Защита интеллектуальной собственности Законодательство РФ в области информационной безопасности	Пр21 Реализация методов стеганографии и криптографии для защиты данных, хранящихся в файлах любого формата.	2
22.		Пр22 Реализация методов стеганографии и криптографии для защиты данных, хранящихся в файлах любого формата.	2
23.		Пр23 Реализация методов стеганографии и криптографии для защиты данных, хранящихся в файлах любого формата.	2
		Итого:	**46**

Раздел 1. Эволюция подходов к обеспечению ИБ

Тема 1.2. Физические и организационные угрозы. Виды мер обеспечения информационной безопасности защита от несанкционированного доступа

Практическая работа №1.

Анализ терминов и определений информационной безопасности. ГОСТы и руководящие документы.– 2 ч

Задание Проанализируйте Доктрину ИБ РФ и постройте схему органов государственной власти и местного самоуправления, отвечающих за информационную безопасность. Определите их функциональные обязанности. Сформулируйте положения государственной политики в области обеспечения информационной безопасности, определите первоочередные мероприятия по обеспечению информационной безопасности, дайте им оценку.

Алгоритм действий

Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. Настоящая Доктрина служит основой для:

- Формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- Подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- Разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Настоящая Доктрина развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере.

1. Информационная безопасность

Российской федерации

1. Методы обеспечения информационной

Безопасности российской федерации

1. Основные положения государственной

Политики обеспечения информационной безопасности российской федерации и первоочередные мероприятия по ее реализации

1. Организационная основа

Системы обеспечения информационной безопасности российской федерации

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя соблюдение конституционных прав и свобод