Министерство науки и высшего образования Российской Федерации
Нижнетагильский государственный социально-педагогический институт (филиал)
федерального государственного автономного образовательного учреждения
высшего образования
«Российский государственный профессионально-педагогический университет»

Факультет естествознания, математики и информатики
Кафедра информационных технологий

УТВЕРЖДАЮ
Зам. директора по УМР
_____ Л. П. Филатова
«____»_____2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.05.04 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень высшего образования	Бакалавриат
Направления подготовки	09.03.03 Прикладная информатика
Профиль	Прикладная информатика в управлении IT-проектами
Формы обучения	Очная, заочная

Нижний Тагил
2019

Рабочая программа дисциплины «Информационная безопасность». Нижний Тагил : Нижнетагильский государственный социально-педагогический институт (филиал) ФГАОУ ВО «Российский государственный профессионально-педагогический университет», 2019. – 15 с.

Настоящая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.03 Прикладная информатика.

Автор: кандидат педагогических наук, Е. С. Васева
доцент кафедры информационных технологий

Рецензент: к.п.н., зам директора по ИТ НТ МУП Д. В. Виноградов
«Нижнетагильские тепловые сети»

Одобрена на заседании кафедры информационных технологий 10 июня 2019 г., протокол № 12.

Заведующая кафедрой ИТ М. В. Мащенко

Одобрена на заседании кафедры информационных технологий 16 мая 2019 г., протокол № 9.

Заведующая кафедрой М. В. Мащенко

Рекомендована к печати методической комиссией факультета естествознания, математики и информатики 21 июня 2019 г., протокол № 10.

Председатель методической комиссии ФЕМИ В.А. Гордеева

Декан ФЕМИ Т. В. Жуйкова

Главный специалист ОИР О. В. Левинских

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины **– формирование компетенций в области обеспечения информационной безопасности в процессе решения профессиональных задач.**

Задачи:

1. Раскрыть понятийный аппарат курса и сформировать целостную систему знаний о современных моделях обеспечения безопасности управления информационными ресурсами.

2. Познакомить студентов с правовыми основами обеспечения информационной безопасности и технологиями обеспечения информационной безопасности средствами систем обеспечения безопасности информации.

3. Сформировать умения решать стандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности.

4. Показать основные направления в управлении информационной безопасностью на предприятии.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Информационная безопасность» является частью учебного плана по направлению подготовки 09.03.03 Прикладная информатика. Дисциплина включена в Блок Б.1 «Дисциплины (модули)» и является составной частью раздела Б1.О. «Обязательная часть». Реализуется кафедрой информационных технологий.

Дисциплина базируется на компетенциях, полученных при изучении дисциплин «Информатика и программирование», «Информационные системы и технологии», «Теория систем и системный анализ», «Операционные системы» и ряда других дисциплин.

3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина направлена на формирование следующих компетенций: ОПК-3, ПК-8.

Код и наименование универсальной компетенции	**Код и наименование индикатора достижения универсальной компетенции**
ОПК-3 – Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ОПК-3.3. Умеет готовить обзоры, аннотации, рефераты, научные доклады, публикации, и библиографию по научно-исследовательской работе с учетом требований информационной безопасности
ПК-8 – Способен принимать участие в организации ИТ- инфра-	ПК-8.1. Знает основы информационной безопасности при организации ИТ инфраструктуры

Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальной компетенции
структуры и управлении информационной безопасностью	ПК-8.2. Знает основные возможности и правила для организации ИТ инфраструктуры предприятия
	ПК-8.3.Умеет создать безопасную ИТ инфраструктуру предприятия

В результате освоения дисциплины обучающийся должен:

знать:

З1. основные понятия курса.

З2. административное и организационно-правовое обеспечение защиты информации.

З3. основные методологические положения защиты информации.

З4. основные сервисы современных информационных систем обеспечения информационной безопасности.

З5. основные программно-аппаратные средства защиты цифровой информации.

З6. особенности работы с антивирусными программами.

З7. достоинства и недостатки, перспективы развития современных систем защиты информации.

уметь:

У1. ограничивать использование ресурсов компьютера на основе раздельного доступа пользователей в операционную систему.

У2. организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа.

У3. организовывать безопасную работу в Интернет.

У4. выполнять резервное копирование, восстановление данных в различных информационных системах.

У5. использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов.

владеть навыками:

В1. установки и настройки сервисов программного обеспечения.

В2. анализа деятельности организации на соответствие нормативно-правовым актам в области информационной безопасности.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Объем дисциплины и виды контактной и самостоятельной работы

Общая трудоемкость дисциплины составляет 3 зач. ед. (108 часов), их распределение по видам работ представлено в таблице.

Распределение трудоемкости дисциплины по видам работ

Вид работы	Кол-во часов	
	Форма обучения	
	очная	заочная
Общая трудоемкость дисциплины по учебному плану	**108**	**108**
Контактная работа, в том числе:	**38**	**10**

Лекции	12	4
Лабораторные занятия	26	6
Самостоятельная работа, в том числе:	**70**	**98**
Самоподготовка к текущему контролю знаний	61	94
Подготовка к зачету	9	4

4.2. Тематический план очной формы обучения

Наименование разделов и тем дисциплины (модуля)	Всего часов	Вид контактной работы, час		Самостоятельная работа, час	Формы текущего контроля успеваемости
		Лекции	Лаб. работы		
Тема 1. Введение в проблему информационной безопасности	10	2		8	
Тема 2. Угрозы информационной безопасности и методы их реализации	12	2	2	8	тест, отчет по лабораторной работе
Тема 3. Правовые аспекты защиты информации	14	2	4	8	тест, отчет по лабораторной работе
Тема 4. Административный уровень обеспечения информационной безопасности	20	2	6	12	тест, отчет по лабораторной работе
Тема 5. Программно-технический уровень обеспечения информационной безопасности	43	4	14	25	тест, отчет по лабораторной работе
Зачет	9	0	0	9	
Итого	**108**	**12**	**26**	**70**	

4.3. Тематический план заочной формы обучения

Наименование разделов и тем дисциплины (модуля)	Всего часов	Вид контактной работы, час		Самостоятельная работа, час	Формы текущего контроля успеваемости
		Лекции	Лаб. работы		
Тема 1. Введение в проблему информационной безопасности	10	0,5		9,5	
Тема 2. Угрозы информационной безопасности и методы их реализации	12	0,5	1	10,5	тест, отчет по лабораторной работе

Наименование разделов и тем дисциплины (модуля)	Всего часов	Вид контактной работы, час		Самостоятельная работа, час	Формы текущего контроля успеваемости
		Лекции	Лаб. работы		
Тема 3. Правовые аспекты защиты информации	14	1	1	12	тест, отчет по лабораторной работе
Тема 4. Административный уровень обеспечения информационной безопасности	25	1	1	23	тест, отчет по лабораторной работе
Тема 5. Программно-технический уровень обеспечения информационной безопасности	43	1	3	39	тест, отчет по лабораторной работе
Зачет	4	0	0	4	ответ на зачете
Итого	**108**	**4**	**6**	**98**	

4.5. Содержание тем дисциплины

Тема 1. Введение в проблему информационной безопасности.

Программа информационной безопасности России и пути ее реализации. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ. Концепция информационной безопасности. Обзор состояния систем защиты информации в России и в ведущих зарубежных странах. Международные стандарты информационного обмена. Основные принципы защиты информации в компьютерных системах. Основные понятия и определения защиты информации.

Тема 2. Угрозы информационной безопасности и методы их реализации.

Виды возможных нарушений информационной системы. Понятие угрозы. Анализ угроз безопасности информации. Причины, виды, каналы утечки и искажения информации. Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации. Информационная безопасность в условиях функционирования в России глобальных сетей.

Тема 3. Правовые аспекты защиты информации.

Современное состояние правового регулирования в информационной сфере. Правовое обеспечение информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, защиты персональных данных, защиты коммерческой тайны, электронной подписи. Стандарты в области информационной безопасности. Компьютерные преступления.

Тема 4. Административный уровень обеспечения информационной безопасности.

Основные понятия. Концепция безопасности. Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом систем. Анализ рисков информационной системы предприятия. Стратегии управления рисками. Частная модель угроз информационной безопасности. Управление персоналом.

Тема 5. Программно-технический уровень обеспечения информационной безопасности.

Основные сервисы программно-технического уровня обеспечения информационной безопасности. Идентификация и аутентификация. Парольная аутентификация. Логическое

управление доступом. Компьютерные вирусы, классификация. Признаки заражения компьютера вредоносным программным обеспечением. Средства защиты от компьютерных вирусов. Протоколирование и аудит. Криптографические средства защиты. Экранирование.

4.5. Практические занятия очной формы обучения

Тема занятия	Количество часов (очная форма обучения)
1. Анализ угроз информационной безопасности.	2
2. Анализ основных нормативных документов в области информационной безопасности.	4
3. Политика информационной безопасности организации. Частная модель угроз	4
4. Разработка локальных нормативных документов	2
5. Обеспечение безопасности при работе с документами	2
6. Возможности защиты информации в операционной системе. Логическое управление доступом	2
7. Основные признаки присутствия на компьютере вредоносных программ	2
8. Установка и предварительная настройка антивирусной программы	2
9. Работа с реестром	2
10. Протоколирование в ИС	2
11. Методы криптографии	2

4.6. Практические занятия заочной формы обучения

Тема занятия	Количество часов (очная форма обучения)
1. Анализ угроз информационной безопасности.	1
2. Анализ основных нормативных документов в области информационной безопасности.	1
3. Политика информационной безопасности организации. Частная модель угроз	1
4. Возможности защиты информации в операционной системе. Логическое управление доступом	1
5. Основные признаки присутствия на компьютере вредоносных программ	1
6. Установка и предварительная настройка антивирусной программы	1

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Представленный курс предусматривает наличие теоретических лекционных занятий, на которых студенты знакомятся с фундаментальными основами и принципами защиты информации на современном этапе развития информационных технологий студенты формируют навыки безопасной работы с различными видами информации.

Основными методами, используемыми при объяснении теоретического материала, являются:

– активные лекции;

– лекции с использованием презентаций;

– лекции с использованием демонстрационных материалов.

Основными методами, используемыми для практических занятий, являются:

– практикум с использованием демонстрационных примеров.

6. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

6.1. Организация самостоятельной работы студентов очной формы обучения

Темы занятий	Количество часов			Содержание самостоятельной работы	Формы контроля СРС
	Всего	Аудиторных	Самостоят. Работы		
Тема 1. Введение в проблему информационной безопасности	10	2	8	Самостоятельное изучение теоретических вопросов – п.1,2 (список прилагается), подготовка тезисов по изученному материалу. Подготовка к тесту	Обсуждение тезисов, тест
Тема 2. Угрозы информационной безопасности и методы их реализации	12	4	8	Самостоятельное изучение теоретического вопроса – п.5 (список прилагается). Подготовка таблицы по видам угроз информационной безопасности. Подготовка к тесту.	Проверка таблицы по видам угроз информационной безопасности. Обсуждение на занятии. Тест
Тема 3. Правовые аспекты защиты информации	14	6	8	Самостоятельное изучение теоретических вопросов – п.3,4 (список прилагается), подготовка тезисов по изученному материалу. Подготовка к лабораторному занятию. Выполнение домашней работы №1. Подготовка к тесту	Обсуждение тезисов, отчет по лабораторной работе, тест
Тема 4. Административный уровень обеспечения информационной безопасности	20	8	12	Подготовка к лабораторной работе, тесту	Отчет по лабораторной работе, тест
Тема 5. Программно-технический уровень обеспечения информационной безопасности	43	18	25	Выполнение домашней работы №2, 3. Подготовка к лабораторной работе, тесту	Обсуждение домашней работы. Отчёт по лабораторной работе, тест
Зачет	9		9	Подготовка к зачету	Ответ на зачете
Всего	**108**	**62**	**70**		

6.2. Организация самостоятельной работы студентов заочной формы обучения

Темы занятий	Количество часов			Содержание самостоятельной работы	Формы контроля СРС
	Всего	Аудиторных	Самостоят. Работы		
Тема 1. Введение в проблему информационной безопасности	10	0,5	9,5	Самостоятельное изучение теоретических вопросов – п.1,2 (список прилагается), подготовка тезисов по изученному материалу. Подготовка к тесту	Обсуждение тезисов, тест
Тема 2. Угрозы информационной безопасности и методы их реализации	12	1,5	10,5	Самостоятельное изучение теоретического вопроса – п.5 (список прилагается). Подготовка таблицы по видам угроз информационной безопасности. Подготовка к тесту.	Проверка таблицы по видам угроз информационной безопасности. Обсуждение на занятии. Тест
Тема 3. Правовые аспекты защиты информации	14	2	12	Самостоятельное изучение теоретических вопросов – п.3,4 (список прилагается), подготовка тезисов по изученному материалу. Подготовка к лабораторному занятию. Выполнение домашней работы №1. Подготовка к тесту	Обсуждение тезисов, отчет по лабораторной работе, тест
Тема 4. Административный уровень обеспечения информационной безопасности	25	2	23	Подготовка к лабораторной работе, тесту	Отчет по лабораторной работе, тест
Тема 5. Программно-технический уровень обеспечения информационной безопасности	43	4	39	Выполнение домашней работы №2, 3. Подготовка к лабораторной работе, тесту	Обсуждение домашней работы. Отчёт по лабораторной работе, тест
Зачет	4		4	Подготовка к зачету	Ответ на зачете
Всего	**108**	**10**	**98**		

6.3. Задания и методические указания по организации самостоятельной работы

Список вопросов, выносимых на самостоятельное изучение

1. История развития систем защиты информации.

2. Обзор состояния систем защиты информации в России и в ведущих зарубежных странах.

3. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

4. Компьютерные преступления.

5. Основные методы реализации угроз информационной безопасности.

Задания для самостоятельной работы (домашние задания)

В рамках самостоятельной работы студентов предусмотрено выполнение творческих домашних заданий. Их цель – закрепление знаний, полученных на практических занятиях.

Домашнее задание №1.

Найти и проанализировать статистических данные об атаках, которым подвергаются компьютерные системы и потерях банков.

Домашнее задание №2.

Проанализировать компьютерные средства реализации защиты в информационных системах вуза, выявить недостатки и предложить пути их решения.

Домашнее задание №3.

Выполнить анализ эффективности 2-3 антивирусных программ.

Домашнее задание №4.

- На основе схемы жизненного цикла криптографических ключей по стандарту ISO/IEC 11770 покажите схемы жизненного цикла секретных и открытых ключей асимметричных криптосистем. Чем они различаются?

- На основе схемы жизненного цикла криптографических ключей по стандарту ISO/IEC 11770 покажите схемы жизненного цикла общих секретных ключей симметричных криптосистем и персональных секретных ключей асимметричных криптосистем. Чем они различаются?

- Предположим, что, используя доступные на сегодняшний день на рынке аппаратные компоненты, возможно собрать компьютер стоимостью около 200 долларов США, который осуществляет опробование около 1 миллиарда ключей алгоритма ГОСТ Р 34.12-2015 в секунду. Предполагая, что конкуренты (или злоумышленники) хотят осуществить поиск одного 256-битного ключа алгоритма ГОСТ Р 34.12-2015 методом тотального опробования и имеют возможность потратить на закупку техники около 4 триллионов долларов США (что на самом деле превышает годовой бюджет США), рассчитайте, какое время займет (в среднем) тотальное опробование для поиска одного 256битного ключа с использованием закупленной техники? (Дополнительные расходы, такие как электроэнергия и тех. поддержка, не принимаются во внимание).

Домашнее задание №5.

Составить схему классификации систем цифровой стеганографии.

Домашнее задание №6.

Перечислите наиболее важные факторы и условия, которые следует учесть при разработке методов по защите информации в информационной среде. Проиллюстрируйте ваш ответ на конкретном примере информационной среды (школа, библиотека, ваша семья, супермаркет, кинотеатр, любая другая среда на ваш выбор).

6.4. Организация текущего контроля и промежуточной аттестации

Качество усвоения учебного материала осуществляется по результатам выполнения заданий для самостоятельной работы на занятии, домашних работ. Особое место в контроле качества занимают отчеты по вопросам, выносимым на самостоятельное изучение. Целесообразно использование следующих форм текущего контроля:

−промежуточный контроль на практических занятиях для оценки самостоятельной работы студента при подготовке к ним;

–обсуждение результатов работы на занятиях и дома;

По результатам текущего контроля принимается решение на допуск студента к итоговому контролю (зачету с оценкой).

Промежуточная аттестация проводится в форме зачета с оценкой. Перечень обязательных видов работы студента, необходимых для получения допуска к зачету:

- Посещение лекционных занятий.

- Ответы на теоретические вопросы на лабораторных занятиях.

- Решение практических задач на лабораторных занятиях, выполнение заданий для самостоятельной работы.

- Выполнение домашних работ.

Критерии оценки:

«Отлично» выставляется студентам, успешно сдавшим экзамен и показавшим глубокое знание теоретической части курса, умение проиллюстрировать изложение практическими примерами, пра-вильно и без ошибок выполнивших практическое задание.

«Хорошо» выставляется студентам, сдавшим экзамен с незначительными замечаниями, показавшим глубокое знание теоретического вопроса, умение проиллюстрировать изложение практическими примерами, выполнившим практическое задание в целом верно, допустившим незначительные ошибки, указывающие на наличие несистематичности и пробелов в знаниях.

«Удовлетворительно» выставляется студентам, сдавшим экзамен со значительными замечаниями, показавшим знание основных положений теории при наличии существенных пробелов, испытывающим затруднения при выполнении практической работы.

«Неудовлетворительно» выставляется, если студент показал существенные пробелы в знаниях основных положений теории, не умеет применять теоретические знания на практике, не выполнил практическое задание.

Примерные теоретические вопросы

1. Проблема информационной безопасности. Основные понятия.
2. Угрозы информационной безопасности.
3. Уровни обеспечения информационной безопасности.
4. Правовое обеспечение информационной безопасности. Основные нормативные документы.
5. ФЗ «О персональных данных».
6. Концепция информационной безопасности предприятия.
7. Политика информационной безопасности предприятия.
8. Анализ рисков информационной системе предприятия.
9. Стратегии управления рисками.
10. Процедурные меры обеспечени информационной безопасности.
11. Основные сервисы программно-технического уровня обеспечения информационной безопасности.
12. Идентификация и аутентификация.
13. Парольная аутентификация.
14. Биометрическая аутентификация.
15. Логическое управление доступом.
16. Компьютерные вирусы, классификация.
17. Признаки заражения компьтера вредоносным программным обеспечением.
18. Средства защиты от компьютерных вирусов.
19. Протоколирование и аудит.
20. Экранирование.
21. Классификация криптографических систем.

22. Симметричные алгоритмы шифрования.
23. Асимметричные алгоритмы шифрования.
24. Криптографические протоколы.
25. Электронная цифровая подпись.
26. Защита информации в сервисах электронных платежей.
27. Криптоанализ и атаки на криптосистемы.
28. Классическая стеганография.
29. Компьютерная стеганография.
30. Удаленные угрозы в вычислительных сетях.
31. Принципы защиты распределенных вычислительных сетей.

Примерные практические задания

Задание 1.

Составьте шаблон документа «Согласие на обработку персональных данных». Выбор реквизитов обоснуйте положениями 152-ФЗ «О персональных данных»

Задание 2.

Разработайте кроссворд по основным понятиям информационной безопасности. Установите пароль на изменение файла, пользователь, имеющий право на изменение может вносить записи только в ячейки кроссворда, не изменяя структура и формулировку вопросов. Установите пароль на открытие файла. Добавьте видимую цифровую подпись к документу.

Задание 3.

В программе Microsoft Excel создайте тест (4-5 вопросов) по теоретическим основам информатики. При вводе правильного ответа соответствующая ячейка должна загораться зеленым цветом. Организуйте защиту файла таким образом, чтобы отвечающему не были доступны сведения, необходимые для проверки ответов.

Задание 4.

С официального сайта GoogleChrome скачайте и установите плагин, позволяющий настроить белый список сайтов, настройте его для работы школьников по теме «Алгоритмизация и программирование», при анализе информационных ресурсов используйте федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию».

Задание 5.

Создайте нового пользователя «Бухгалтер» в операционной системе, назначьте ему группу пользователя, выбор обоснуйте. Для пользователя «Бухгалтер» настройте главное меню и рабочий стол так, чтобы доступ открывался только к рабочим файлам, настройки осуществляйте с учетной записи администратора.

Задание 6.

Выберите и установите на компьютер утилиту, позволяющую осуществить чистку реестра компьютера. Отключите автозапуск программ, обоснуйте выбор отключаемых программ. Найдите на компьютере все файлы дубликаты.

Задание 7.

Выберите и установите на компьютер антивирусное программное обеспечение. Выполните следующие настройки:

- Установить пароль, сделать общедоступными «Общий доступ к программе» и «Контроль обновлений», все остальные варианты включить в защиту.

- Добавить в исключения сайт https://www.ntspi.ru/ , а в усиленный режим сканирования добавить одну из программ, установленных на компьютере.

- Настроить выгрузку отчетов для веб-экранов в формате HML , в отчет включить: зараженные файлы, серьезные ошибки и файлы, не прошедшие проверку.

- Ограничить доступ с компьютера к трем сайтам. Попробовать перейти на эти сайты.

- Просканировать одну из папок, находящуюся на компьютере.

Задание 8.

Одна фирма предложила устройство для автоматической проверки пароля. Паролем может быть любой непустой упорядоченный набор букв в алфавите *{a, b, c}*. Будем обозначать такие наборы большими латинскими буквами. Устройство перерабатывает введенный в него набор *P* в набор *Q = F(P)*. Отображение *F* держится в секрете, однако про него известно, что оно определено не для каждого набора букв и обладает следующими свойствами. для любого набора букв *P*

1) *F(aP) = P*;

2) *F (bP) = F (P)a F(P)*;

3) набор *F(cP)* получается из набора *F(P)* переписыванием его букв в обратном порядке.

Устройство признает предъявленный пароль верным, если *F(P) =P*. Например, трехбуквенный набор *bab*является верным паролем, так как *F(bab) = F(ab) a F(ab) = bab*.

Подберите верный пароль, состоящий более чем из трех букв.

Задание 9.

Злоумышленник хочет получить доступ к банковской ячейке, защищенной кодовым замком. Комбинация из трех цифр (u,v,w), отпирающая замок, ему не известна. Злоумышленнику удалось изготовить проксимити-карты со следующей информацией: на первой карте записаны цифры (1,5,8), на второй – (7,4,9), на третьей – (9,7,6), на четвертой – (3,2,4). При прикладывании карты с информацией (a,b,c) к считывающему устройству банковской ячейки, ее кодовый замок из состояния (i,j,k) переходит в состояние (i+a,j+b,k+c). (Если какая-либо сумма превосходит 9, то она заменяется ее остатком от деления на 10.) Как только замок оказывается в состоянии (u,v,w), он немедленно открывается. Какое наименьшее количество из имеющихся карт следует использовать, чтобы гарантированно открыть ячейку, независимо от установленной отпирающей комбинации (u,v,w) и начального состояния замка?

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Основная литература

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/434171 (дата обращения: 16.03.2019). — Режим доступа: для авториз. пользователей.

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/432966 (дата обращения: 16.03.2019). — Режим доступа: для авториз. пользователей.

Дополнительная литература

3. Акмаров, П. Б. Кодирование и защита информации : учебное пособие / П. Б. Акмаров. — Ижевск : Ижевская ГСХА, 2016. — 136 с. — Текст : электронный // Лань : элек-

тронно-библиотечная система. — URL: https://e.lanbook.com/book/133975 (дата обращения: 16.03.2019). — Режим доступа: для авториз. пользователей.

4. Бондаренко, И. С. Методы и средства защиты информации : учебное пособие / И. С. Бондаренко, Ю. В. Демчишин. — Москва : МИСИС, 2018. — 32 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/115269 (дата обращения: 16.03.2019). — Режим доступа: для авториз. пользователей.

5. Васильев, В. И. Интеллектуальные системы защиты информации : учебное пособие / В. И. Васильев. — 2-е изд., испр. и доп. . — Москва : Машиностроение, 2013. — 172 с. — ISBN 978-5-94275-667-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5792 (дата обращения: 16.03.2019). — Режим доступа: для авториз. пользователей.

6. Исаева, М. Ф. Техническая защита информации : учебное пособие / М. Ф. Исаева. — Санкт-Петербург : ПГУПС, 2017. — 49 с. — ISBN 978-5-7641-1008-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/101600 (дата обращения: 16.03.2019). — Режим доступа: для авториз. пользователей.

7. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/441287 (дата обращения: 16.03.2019). — Режим доступа: для авториз. пользователей.

8. Милославская, Н. Г. Серия «Вопросы управление информационной безопасностью". Выпуск 2 : учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 130 с. — ISBN 978-5-9912-0272-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5179 (дата обращения: 16.03.2019). — Режим доступа: для авториз. пользователей.

9. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2019. — 96 с. — ISBN 978-5-8114-4040-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114697 (дата обращения: 16.03.2019). — Режим доступа: для авториз. пользователей.

10. Технические средства и методы защиты информации : учебное пособие / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков, И. В. Голубятников. — Москва : Горячая линия-Телеком, 2012. — 616 с. — ISBN 978-5-9912-0084-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5154 (дата обращения: 16.03.2019). — Режим доступа: для авториз. пользователей.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебная аудитория 213А: 11 посадочных мест для студентов, рабочее место преподавателя, компьютеры – 12 шт., маркерная доска, проекционное оборудование.

Программное обеспечение

Браузер Google chrome/Mozilla Firefox;
Microsoft Office/ OpenOffice/ LibreOffice;
Oracle VirtualBox;
ОС GNU/Linux;
Packet Tracer.