Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 17.02.2023 11:49:24
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / Д.Г. Демидов /
«16» 02 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информационная безопасность и защита информации»

Направление подготовки/специальность

09.03.02 Информационные системы и технологии

Профиль/специализация

Автоматизированные системы обработки информации и управления
Информационные системы умных пространств
Информационные технологии в медиаиндустрии и дизайне
Программное обеспечение игровой компьютерной индустрии
Технологии дополненной и виртуальной реальности
Цифровая трансформация

Квалификация

Бакалавр

Формы обучения

Очная, заочная

Москва, 2023 г.

Разработчик(и):
доцент, к.т.н. /М.А.Иванько /

Согласовано:

Заведующий кафедрой «Информатики и информационных технологий», к.т.н. _____ /Е.В. Булатников/

Содержание

1. Цели и задачи дисциплины: 4
2. Место дисциплины в структуре ОП 4
3. Структура и содержание дисциплины 5
3.1 Виды учебной работы и трудоемкость 5
3.2 Тематический план изучения дисциплины 6
3.3 Содержание дисциплины 7
3.4 Тематика семинарских/практических и лабораторных занятий 8
3.5 Тематика курсовых проектов (курсовых работ) 10
4. Учебно-методическое и информационное обеспечение 10
4.1 Нормативные документы и ГОСТы 10
4.2 Основная литература 10
4.3 Дополнительная литература 11
4.4 Электронные образовательные ресурсы 11
4.5 Лицензионное и свободно распространяемое программное обеспечение 11
4.6 Современные профессиональные базы данных и информационные справочные системы 11
5. Материально-техническое обеспечение 11
6. Методические рекомендации 11
6.1 Методические рекомендации для преподавателя по организации обучения 11
6.2 Методические указания для обучающихся по освоению дисциплины 12
7. Фонд оценочных средств 12
7.1 Методы контроля и оценивания результатов обучения 12
7.2 Шкала и критерии оценивания результатов обучения 12
7.3 Оценочные средства 16

1. Цели и задачи дисциплины:

Целью освоения дисциплины «Информационная безопасность и защита информации» является знакомство обучающихся с основными алгоритмами и методами защиты информации, а также применение различных подходов к защите информации на практике.

Задачи дисциплины:

- изучение современных алгоритмов шифрования информации;
- изучение современных алгоритмов хэширования;
- изучение вирусов и методов борьбы с ними;
- изучение вопросов социальной инженерии;
- изучение методов построения комплексной системы безопасности.

2. Место дисциплины в структуре ОП

Дисциплина «Информационная безопасность и защита информации» относится к обязательной части Блока 1 «Дисциплины (модули)» учебного плана программы бакалавриата по направлению 09.03.02 «Информационные системы и технологии».

Изучение данной дисциплины базируется на следующих дисциплинах:

- Базы данных
- Сети телекоммуникации
- Растровая и векторная графика
- Операционные системы
- Инструменты визуализации данных
- Проектирование интерфейсов информационных систем
- Офисные приложения
- Теория информации
- Аппаратное обеспечение информационных систем
- Системы управления разработкой программного обеспечения

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих за ней дисциплин, практик:

- Управление программными проектами
- Преддипломная практика
- Государственная итоговая аттестация (выполнение и защита ВКР)

Требования к результатам освоения дисциплины

Код компетенции	**Наименования компетенции**	**Индикаторы достижение 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	ИОПК-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 ИОПК-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 ИОПК-3.3. имеет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

3. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

3.1 Виды учебной работы и трудоемкость

п/п	**Вид учебной работы**	**Количество часов**	**Семестры**
			6
	Аудиторные занятия	**54**	54
	В том числе:		
1.	Лекции	18	18
2.	Семинарские/практические занятия		
3.	Лабораторные занятия	36	36
	Самостоятельная работа	**54**	54
	Промежуточная аттестация		
	Зачет/диф.зачет/экзамен	**зачет**	зачет
	Итого	**108**	

3.2 Тематический план изучения дисциплины

Разделы/темы дисциплины	Трудоемкость, час					
	Всего	Аудиторная работа				Самостоятельная работа
		Лекции	Семинарские/практические	Лабораторные занятия	Практическая подготовка	
Тема 1. Понятие "информационная» безопасность и уровни ее обеспечения. Проблема информационной безопасности общества. Определение понятия "информационная безопасность"	7	1		2		4
Тема 2. Составляющие информационной безопасности. Доступность информации. Целостность информации. Конфиденциальность информации	7	1		2		4
Тема 3. Система формирования режима информационной безопасности. Задачи информационной безопасности общества. Уровни формирования режима информационной безопасности	7	1		2		4
Тема 4. Нормативно-правовые основы информационной безопасности в РФ. Правовыеосновы информационной безопасности общества. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности	12	2		4		6
Тема 5. Стандарты информационной безопасности: "Общие критерии". Требования безопасности к информационным системам. Принцип иерархии: класс – семейство – компонент – элемент. Функциональные требования. Требованиядоверия	12	2		4		6
Тема 6. Стандарты информационной безопасности распределенных систем. Сервисы безопасности в вычислительных сетях. Механизмы безопасности. Администрирование средств безопасности	10	2		4		4
Тема 7. Стандарты информационной безопасности в РФ. Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ. Документы по оценке защищенности автоматизированных систем в РФ	12	2		4		6

Тема 8. Административный уровень обеспечения информационной безопасности. Цели, задачи и содержание административного уровня. Разработка политики информационной безопасности	10	2		4		4
Тема 9. Классификация угроз "информационной безопасности". Классы угроз информационной безопасности. Каналы несанкционированного доступа к информации	7	1		2		4
Тема 10. Компьютерные вирусы и защита от них. Вирусы как угроза информационной безопасности. Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов. Классификация компьютерных вирусов. Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по особенностям алгоритма работы. Классификация компьютерных вирусов по деструктивным возможностям	12	2		4		6
Тема 11. Антивирусные программы. Особенности работы антивирусных программ. Классификация антивирусных программ. Факторы, определяющие качество антивирусных программ. Профилактика компьютерных вирусов. Характеристика путей проникновения вирусов в компьютеры. Правила защиты от компьютерных вирусов	12	2		4		6
Итого:	**108**	**18**		**36**		**54**

3.3 Содержание дисциплины

Тема 1.

Понятие "информационная» безопасность и уровни ее обеспечения.

. Проблема информационной безопасности общества. Определение понятия"информационная безопасность".

Тема 2.

Составляющие информационной безопасности. Доступность информации.Целостность информации. Конфиденциальность информации.

Тема 3.

Система формирования режима информационной безопасности. Задачи информационной безопасности общества. Уровни формирования режимаинформационной безопасности.

Тема 4.

Нормативно-правовые основы информационной безопасности в РФ. Правовыеосновы информационной безопасности общества. Основные

положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности.

Тема 5.

Стандарты информационной безопасности: "Общие критерии". Требования безопасности к информационным системам. Принцип иерархии: класс – семейство – компонент – элемент. Функциональные требования. Требованиядоверия.

Тема 6.

Стандарты информационной безопасности распределенных систем. Сервисыбезопасности в вычислительных сетях. Механизмы безопасности. Администрирование средств безопасности.Тема 7.

Стандарты информационной безопасности в РФ. Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ.Документы по оценке защищенности автоматизированных систем в РФ.

Тема 8.

Административный уровень обеспечения информационной безопасности. Цели,задачи и содержание административного уровня. Разработка политики информационной безопасности.

Тема 9.

Классификация угроз "информационной безопасности". Классы угроз информационной безопасности. Каналы несанкционированного доступа кинформации.

Тема 10.

Компьютерные вирусы и защита от них. Вирусы как угроза информационнойбезопасности. Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов. Классификация компьютерных вирусов. Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по особенностям алгоритма работы. Классификация компьютерных вирусов по деструктивным возможностям.

Тема 11.

Антивирусные программы. Особенности работы антивирусных программ. Классификация антивирусных программ. Факторы, определяющие качество антивирусных программ. Профилактика компьютерных вирусов. Характеристикапутей проникновения вирусов в компьютеры. Правила защиты от компьютерныхвирусов.

3.4 Тематика семинарских/практических и лабораторных занятий

Семинарские/практические занятия по данной дисциплине не предусмотрены.

Лабораторная работа 1.
Понятие "информационная» безопасность и уровни ее обеспечения.
. Проблема информационной безопасности общества. Определение понятия"информационная безопасность".
Лабораторная работа 2.
Составляющие информационной безопасности. Доступность информации.Целостность информации. Конфиденциальность информации.
Лабораторная работа 3.
Система формирования режима информационной безопасности. Задачи информационной безопасности общества. Уровни формирования режимаинформационной безопасности.
Лабораторная работа 4.
Нормативно-правовые основы информационной безопасности в РФ. Правовыеосновы информационной безопасности общества. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности.
Лабораторная работа 5.
Стандарты информационной безопасности: "Общие критерии". Требования безопасности к информационным системам. Принцип иерархии: класс – семейство – компонент – элемент. Функциональные требования. Требованиядоверия.
Лабораторная работа 6.
Стандарты информационной безопасности распределенных систем. Сервисыбезопасности в вычислительных сетях. Механизмы безопасности.
Администрирование средств безопасности.Лабораторная работа 7.
Стандарты информационной безопасности в РФ. Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ.Документы по оценке защищенности автоматизированных систем в РФ.
Лабораторная работа 8.
Административный уровень обеспечения информационной безопасности. Цели,задачи и содержание административного уровня. Разработка политики информационной безопасности.
Лабораторная работа 9.
Классификация угроз "информационной безопасности". Классы угроз информационной безопасности. Каналы несанкционированного доступа кинформации.
Лабораторная работа 10.
Компьютерные вирусы и защита от них. Вирусы как угроза

информационнойбезопасности. Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов. Классификация компьютерных вирусов. Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по особенностям алгоритма работы. Классификация компьютерных вирусов по деструктивным возможностям.
Лабораторная работа 11.
Антивирусные программы. Особенности работы антивирусных программ. Классификация антивирусных программ. Факторы, определяющие качество антивирусных программ. Профилактика компьютерных вирусов. Характеристикапутей проникновения вирусов в компьютеры. Правила защиты от компьютерныхвирусов.

3.5 Тематика курсовых проектов (курсовых работ)

Курсовые проекты по данной дисциплине не предусмотрены.

4. Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. https://fgos.ru/fgos/fgos-01-03-02-prikladnaya-matematika-i-informatika-9/2. "Положения об организации образовательного процесса в Московском Политехническом университете"

4.2 Основная литература

1. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 с. — ISBN 978-5-4497-0338-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89453.html (дата обращения: 30.09.2023)
2. Фомин, Д. В. Информационная безопасность : учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 54 с. — ISBN 978-5-4487-0298-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/77320.html (дата обращения: 30.09.2023)
3. Защита информации с использованием механизмов электронной цифровой подписи: учебно-метод. пособие / Д.Г. Демидов, О.Г. Швечкова, О.А. Москвитина, А.Н. Пылькин, К.А. Майков, К.Г. Смирнова ; Моск. гос. ун-т печати имени Ивана Федорова. — М. : МГУП имени Ивана Федорова, 2014. — 53 с. [Электронный ресурс] URL: http://elib.mgup.ru/showBook.php?id=99.

4.3 Дополнительная литература

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/97562.html (дата обращения: 30.09.2023)

4.4 Электронные образовательные ресурсы

СДО Московского Политеха. «Информационная безопасность и защита информации». https://online.mospolytech.ru/course/view.php?id=11843

4.5 Лицензионное и свободно распространяемое программное обеспечение

Для успешного освоения дисциплины, студент использует следующие программные средства: среда разработки Android Studio.

4.6 Современные профессиональные базы данных и информационные справочные системы

1. https://elenph.org/
2. https://www.philosophy.ru/
3. https://iphlib.ru/library

5. Материально-техническое обеспечение

Для проведения лекционных занятий используются компьютер и проектор для использования лекционного материала в форме презентационных слайдов, компьютерный класс (не менее 15 посадочных мест) с установленным программным обеспечением для проведения лабораторных работ.

6. Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

Изучение дисциплины «Программирование для мобильных устройств» обучающимися направления подготовки бакалавров 09.03.02 предусмотрено рабочим учебным планом во 2-ом семестре четвёртого года обучения.

Лекционные занятия проводятся в соответствии с содержанием настоящей рабочей программы.

Лабораторные работы по дисциплине «Информационная

безопасность и защита информации» осуществляется в форме самостоятельной проработки теоретического материала обучающимися; выполнения практического задания; защиты преподавателю лабораторной работы (знаниетеоретического материала и выполнение практического задания).

При проведении контрольной точки обучающиеся не менее чем за неделю информируются об этом и им выдается список вопросов для подготовки к контрольной работе.

6.2 Методические указания для обучающихся по освоению дисциплины

Посещение лекционных занятий является обязательным. Пропуск лекционных занятий без уважительных причин и согласования с руководством в объеме более 40% от общего количества предусмотренных учебным планом на семестр лекций влечет за собой невозможность аттестации по дисциплине.

Допускается конспектирование лекционного материала письменным или компьютерным способом.

Регулярная проработка материала лекций по каждому разделу в рамках подготовки к промежуточным и итоговым формам аттестации, а также выполнение и подготовка к защите лабораторных работ по дисциплине является одним из важнейших видов самостоятельной работы обучающегося в течение семестра.

7. Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- подготовка к выполнению лабораторных работ и их защита.

Оценочные средства текущего контроля успеваемости включают контрольные вопросы для контроля освоения обучающимися разделов дисциплины.

Образцы контрольных вопросов и заданий для проведения текущего контроля, экзаменационных билетов, приведены в приложении 1.

7.2 Шкала и критерии оценивания результатов обучения

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

Показатель	Критерии оценивания			
	не зачтено	зачтено		
	2	3	4	5
ИОПК-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	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Обучающийся не владеет или в недостаточной степени освоил знания, умения, навыки, приведённые в таблицах показателей.	Выполнены все виды учебной работы, предусмотренные учебным планом. Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей. Допускаются значительные ошибки, проявляется недостаточность знаний, умений, навыков, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями, умениями, навыками при их переносе на новые ситуации.	Выполнены все виды учебной работы, предусмотренные учебным планом. Обучающийся демонстрирует частичное соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные	Выполнены все виды учебной работы, предусмотренные учебным планом. Обучающийся демонстрирует частичное соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые,

			ситуации.	нестандартные ситуации.
ИОПК-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	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Обучающийся не владеет или в недостаточной степени освоил знания, умения, навыки, приведённые в таблицах показателей.	Выполнены все виды учебной работы, предусмотренные учебным планом. Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей. Допускаются значительные ошибки, проявляется недостаточность знаний, умений, навыков, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями, умениями, навыками при их переносе на новые ситуации.	Выполнены все виды учебной работы, предусмотренные учебным планом. Обучающийся демонстрирует частичное соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.	Выполнены все виды учебной работы, предусмотренные учебным планом. Обучающийся демонстрирует частичное соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

ИОПК-3.3. Имеет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Обучающийся не владеет или в недостаточной степени освоил знания, умения, навыки, приведённые в таблицах показателей.	Выполнены все виды учебной работы, предусмотренные учебным планом. Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей. Допускаются значительные ошибки, проявляется недостаточность знаний, умений, навыков, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями, умениями, навыками при их переносе на новые ситуации.	Выполнены все виды учебной работы, предусмотренные учебным планом. Обучающийся демонстрирует частичное соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.	Выполнены все виды учебной работы, предусмотренные учебным планом. Обучающийся демонстрирует частичное соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

Форма промежуточной аттестации: зачёт.

Промежуточная аттестация обучающихся в форме зачёта проводится по результатам выполнения всех видов учебной работы, предусмотренных

учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «зачтено» или «не зачтено».

К промежуточной аттестации допускаются только студенты, выполнившие все виды учебной работы, предусмотренные рабочей программой по дисциплине «Интеллектуальные системы и технологии».

Шкала оценивания	**Описание**
Зачтено	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенных в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях различной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Не зачтено	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенных в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

Вопросы к экзамену по дисциплине «Информационная безопасность и защита информации»

1. Криптография. Основные определения и алгоритмы.
2. Классификация криптоалгоритмов.
3. Симметричные криптоалгоритмы.
4. Скремблеры.
5. Блочные шифры.
6. Сеть Фейштеля. Блочный шифр TEA.
7. Общие сведения о конкурсе AES: шифр MARS
8. Общие сведения о конкурсе AES: шифр RC6
9. Общие сведения о конкурсе AES: шифр Serpent

10. Общие сведения о конкурсе AES: шифр TwoFish
11. Общие сведения о конкурсе AES: шифр Rijndael.
12. Симметричные криптосистемы.
13. Асимметричные криптоалгоритмы.
14. Алгоритм RSA.
15. Обмен ключами по алгоритму Диффи-Хеллмана.
16. Общая схема асимметричной криптосистемы
17. Общие сведения о вирусах.
18. Вирусы под Unix-подобные системы.
19. Классификация вирусов.
20. Классификация вирусов по среде обитания.
21. Классификация вирусов по способам заражения.
22. Классификация вирусов по наносимому вреду.
23. Классификация вирусов по особенностям алгоритма.
24. Классификация вирусов по версии DrWeb.
25. Понятие и классификация антивирусных программ.
26. Обзор современных антивирусных программ.
27. Поиск вирусов вручную.
28. Инструменты для борьбы с вирусами.
29. Понятие социальной инженерии.
30. Мотивы и методы социальной инженерии.
31. Получение конфиденциальной информации.
32. Заражение компьютера вирусом.
33. Инструменты социальной инженерии.
34. Массовые рассылки (известные так же, как спам).
35. Баннеры. Обратная социальная инженерия.
36. Безопасность в интернете
37. Общий обзор угроз, рекомендации по безопасности.
38. Безопасная работа в Интернете: анализ веб-сайтов, безопасный поиск, надежные пароли.
39. Безопасная работа в Интернете: электронная почта, платежи, защитное ПО.
40. Дополнительные средства повышения безопасности.
41. Резервное копирование и шифрование данных, вопросы обеспечения физической безопасности компьютера.
42. Безопасность при работе на компьютере нескольких пользователей.
43. Безопасность в социальных сетях.
44. Концепции и аспекты обеспечения информационной безопасности
45. Понятия экономической и информационной безопасности.
46. Ключевые вопросы ИБ.
47. Виды угроз информационной безопасности и классификация источников угроз.
48. Основные виды защищаемой информации.
49. Правовое обеспечение информационной безопасности.
50. Основные аспекты построения системы информационной безопасности