ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
МИНИСТЕРСТВА СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА ИМЕНИ В.И. ВЕРНАДСКОГО»
(Университет Вернадского)

Кафедра Цифровых систем и инженерных технологий

Принято Ученым советом
Университета Вернадского
«26» сентября 2024 г. протокол №2

«УТВЕРЖДЕНО»
Проректор по образовательной деятельности
_____Кудрявцев М.Г.
«26» сентября 2024 г.

Рабочая программа дисциплины

Информационная безопасность

Направление подготовки 09.04.03 Прикладная информатика

Направленность (профиль) программы Искусственный интеллект и программирование

Квалификация Магистр

Форма обучения **очная**

Балашиха 2024

Рабочая программа разработана в соответствии с ФГОС ВО по направлению подготовки 09.04.03 Прикладная информатика

Рабочая программа дисциплины разработана *доцентом кафедры цифровых систем и инженерных технологий, к.т.н. Рамазановой Г.Г.*

Рецензент: *доцент кафедры цифровых систем и инженерных технологий, к.э.н. Сидоров А.В.*

1. Планируемые результаты обучения по дисциплине, соотнесенные с установленными в ОПОП ВО индикаторами достижения компетенций

1.1 Перечень компетенций, формируемых учебной дисциплиной

Код и наименование компетенции	Индикаторы достижения компетенций Планируемые результаты обучения
Профессиональные компетенции	
ПК-1 Способен выполнять теоретические исследования процессов создания, накопления и обработки информации, включая анализ и создание моделей данных и знаний, языков их описания и манипулирования, разработку новых математических методов и средств поддержки интеллектуальной обработки данных	Знать: основные понятия, виды моделей, современный инструментарий и методы имитационного моделирования, проведение имитационного эксперимента; методы формализации и постановки задач имитационного моделирования Уметь: Использовать информационные технологии имитационного моделирования с использованием современных систем имитационного моделирования; методы разработки математического и программного обеспечения имитационных моделей; современные инструментарий имитационного моделирования. Владеть: Построением процессов и событийных моделей дискретных систем; выполнением формализации и постановки задач имитационного моделирования; разработкой имитационных моделей систем и процессов, планированием и выполнением имитационного эксперимента с использованием систем имитационного моделирования
ПК-2 Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения	Знать: современные методы разработки и реализации алгоритмов математических моделей на базе языков и пакетов прикладных программ моделирования. Уметь: Разработкой и реализацией алгоритмов математических моделей на базе языков и пакетов прикладных программ моделирования. Владеть: в практической деятельности разработкой алгоритмов на базе языков и пакетов прикладных программ моделирования

2. Цели и задачи освоения учебной дисциплины, место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность» относится к обязательной части основной профессиональной образовательной программы высшего образования 09.04.03 Прикладная информатика, профиль «Искусственный интеллект и программирование».

Целями изучения дисциплины «Информационная безопасность» является формирование у обучающихся общекультурных и профессиональных компетенций в процессе изучения различных аспектов защиты информации для последующего применения в учебной и практической деятельности.

Задачи дисциплины:

- систематизация, формализация и расширение знаний по основным положениям теории информации, информационной безопасности и стандартами шифрования;

- изучение математических основ защиты информации; а так же методов, средств и инструментов шифрования, применяемых в сфере информационных технологий и бизнеса;
- дать студенту достаточно прочные представления о информационной безопасности, включая аппаратную часть и математическое обеспечение;
- привитие навыков работы с методами шифрования и криптоанализа;
- формирование современной культуры программирования.

3. Объем учебной дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий, текущий и промежуточный контроль по дисциплине) и на самостоятельную работу обучающихся

Вид учебной работы	2 семестр
Общая трудоемкость дисциплины, зачетных единиц	7
часов	**252**
Аудиторная (контактная) работа, часов	**70,3**
в т.ч. занятия лекционного типа	28
занятия семинарского типа	42
промежуточная аттестация	0,3
Самостоятельная работа обучающихся, часов	**172,7**
Курсовая работа	+
Вид промежуточной аттестации	экзамен

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Перечень разделов дисциплины с указанием трудоемкости аудиторной (контактной) и самостоятельной работы, видов контролей и перечня компетенций

Наименование разделов и тем	Трудоемкость, часов			Код компетенции
	всего	в том числе		
		аудиторной (контактной) работы	самостоятельной работы	
Раздел 1. Основные составляющие информационной безопасности. Криптографические способы защиты информации.	**121**	35	86	ПК-1 ПК-2
Раздел 2. Антивирусная защита. Сетевая безопасность.	**122**	35,3	86,7	
Курсовая работа	+	+	+	
Итого за семестр	**243**	70,3	172,7	
Промежуточная аттестация	9	0,3	-	
ИТОГО по дисциплине	**252**	**70,3**	**172,7**	

2. Содержание дисциплины по разделам

Раздел 1. Основные составляющие информационной безопасности. Криптографические способы защиты информации.

Перечень учебных элементов раздела:

Основные понятия информационной безопасности. Классификация угроз. Классификация средств защиты информации. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности. Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Простые криптосистемы. Шифрование методом замены (подстановки). Одноалфавитная подстановка. Многоалфавитная одноконтурная обыкновенная подстановка. Таблицы Вижинера. Многоалфавитная одноконтурная монофоническая подстановка. Многоалфавитная многоконтурная подстановка. Шифрование методом перестановки. Простая перестановка. Перестановка, усложненная по таблице. Перестанов ка, усложненная по маршрутам. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Общая схема алгоритма IDEA.

Раздел 2. Антивирусная защита. Сетевая безопасность.

Перечень учебных элементов раздела:

Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы. Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты. Уровень защиты рабочих станций и сетевых серверов. Уровень защиты почты. Уровень защиты шлюзов. Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети. Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись. Установление подлинности объекта. Управление ключами. Безопасность на прикладном уровне: PGP и S/MIME. Безопасность на транспортном уровне: SSL и TLS. Безопасность на сетевом уровне: IP SEC. Брандмауэры. Определение типов брандмауэров. Разработка конфигурации межсетевого экрана. Построение набора правил межсетевого экрана. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. Анализаторы системных вызовов. Анализаторы поведения приложений. Контроллеры целостности файлов. Сетевые IDS. Установка IDS. Определение целей применения IDS. Управление IDS.

5. Оценочные материалы по дисциплине

Оценочные материалы по дисциплине представлены в виде фонда оценочных средств.

6. Материально-техническое и учебно-методическое обеспечение дисциплины

6.1 Перечень учебно-методического обеспечения по дисциплине

№ п/п	Автор, название, место издания, издательство, год издания, количество страниц, режим доступа
1	Методические указания по изучению дисциплины

6.2 Перечень учебных изданий, необходимых для освоения дисциплины

Основная литература:

1. Раченко, Т. А. Информационная безопасность : учебно-методическое пособие / Т. А. Раченко. — Тольятти : ТГУ, 2024. — 135 с. — ISBN 978-5-8259-1612-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/427130

2. Информационная безопасность : учебное пособие / составители И. Б. Тесленко [и др.] ; под редакцией И. Б. Тесленко. — Владимир : ВлГУ, 2023. — 212 с. — ISBN 978-5-9984-1783-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/434282

3. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 400 с. — ISBN 978-5-507-49250-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/414947

Дополнительная литература:

1. Давыдов, А. И. Управление информационной безопасностью : учебное пособие / А. И. Давыдов, Д. А. Елизаров. — Омск : ОмГУПС, 2023. — 91 с. — ISBN 978-5-949-41321-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/419255

2. Крыжановский, А. В. Информационная безопасность : методические указания / А. В. Крыжановский, И. С. Поздняк. — Самара : ПГУТИ, 2018. — 38 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182282

6.3 Современные профессиональные базы данных, информационные справочные системы и лицензионное программное обеспечение

Современные профессиональные базы данных, информационные справочные системы, цифровые электронные библиотеки и другие электронные образовательные ресурсы

1. Договор о подключении к Национальной электронной библиотеке и предоставлении доступа к объектам Национальной электронной библиотеки №101/НЭБ/0502-п от 26.02.2020 5 лет с пролонгацией
2. Соглашение о бесплатном тестовом доступе к Polpred.com. Обзор СМИ 27.04.2016 бессрочно
3. Соглашение о бесплатном тестовом доступе к Polpred.com. Обзор СМИ 02.03.2020 бессрочно
4. Информационно-справочная система «Гарант» – URL: https://www.garant.ru/ Информационно-справочная система Лицензионный договор № 261709/ОП-2 от 25.06.2021
5. «Консультант Плюс». – URL: http://www.consultant.ru/ свободный доступ
6. Электронно-библиотечная система AgriLib http://ebs.rgunh.ru/ (свидетельство о государственной регистрации базы данных №2014620472 от 21.03.2014).

Доступ к электронной информационно-образовательной среде, информационно-телекоммуникационной сети «Интернет»

1. Система дистанционного обучения Moodle www.portfolio.rgunh.ru (свободно распространяемое)

2. Право использования программ для ЭВМ Mirapolis HCM в составе функциональных блоков и модулей: Виртуальная комната.

3. Инновационная система тестирования – программное обеспечение на платформе 1С (Договор № К/06/03 от 13.06.2017). Бессрочный.

4. Образовательный интернет – портал Университета Вернадского (свидетельство о регистрации средства массовых информации Эл № ФС77-51402 от 19.10.2012).

Лицензионное и свободно распространяемое программное обеспечение

1. OpenOffice – свободный пакет офисных приложений (свободно распространяемое)
2. linuxmint.com https://linuxmint.com/ (свободно распространяемое)
3. Электронно-библиотечная система AgriLib http://ebs.rgunh.ru/ (свидетельство о государственной регистрации базы данных №2014620472 от 21.03.2014) собственность университета.
4. Официальная страница ФГБОУ ВО МСХ РФ «Российский государственный университет народного хозяйства имени В.И. Вернадского» https://vk.com/rgunh.ru (свободно распространяемое)
5. Портал ФГБОУ ВО МСХ РФ «Российский государственный университет народного хозяйства имени В.И. Вернадского» (свободно распространяемое) https://zen.yandex.ru/id/5fd0b44cc8ed19418871dc31
6. Антивирусное программное обеспечение Dr. WEB Desktop Security Suite (Сублицензионный договор №13740 на передачу неисключительных прав на программы для ЭВМ от 01.07.2021).

6.4 Перечень учебных аудиторий, оборудования и технических средств обучения

Учебная аудитория для проведения лекционных занятий (поточная). Специализированная мебель, доска меловая, мультимедийное оборудование, экран настенный, проектор	143907, Московская область, г. Балашиха, ул. шоссе Энтузиастов, д.50, каб. 235 Площадь помещения 73,4 кв.м № по технической инвентаризации 239, этаж 2
Учебная аудитория для занятий лекционного типа, семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы), для проведения групповых консультаций и индивидуальной работы обучавшихся с педагогическими работниками, для проведения текущего контроля и промежуточной аттестации. Специализированная мебель, доска меловая. Персональные компьютеры в сборке с выходом в интернет.	143907, Московская область, г. Балашиха, ул. шоссе Энтузиастов, д. 50, каб. 142 Площадь помещения 69,1 кв.м № по технической инвентаризации 147, этаж 1
Помещение для самостоятельной работы. Персональные компьютеры в сборке с выходом в интернет.	143907, Московская область, г. Балашиха, ул. шоссе Энтузиастов, д. 50, читальный зал Площадь помещения 497,4 кв. м. № по технической инвентаризации 177, этаж 1
Помещение для самостоятельной работы. Специализированная мебель, персональные компьютеры в сборке с выходом в интернет.	143900, Московская область, г. Балашиха, ул. Юлиуса Фучика д.1, каб. 320 Площадь помещения 49,7 кв. м. № по технической инвентаризации 313, этаж 3

Учебная аудитория для учебных занятий обучающихся из числа инвалидов и лиц с ОВЗ. Специализированная мебель. Автоматизированное рабочее место для инвалидов-колясочников с коррекционной техникой и индукционной системой ЭлСис 290; Автоматизированное рабочее место для слабовидящих и незрячих пользователей со стационарным видеоувеличителем ЭлСис 29 ON; Автоматизированное рабочее место для слабовидящих и незрячих пользователей с портативным видеоувеличителем ЭлСис 207 CF; Автоматизированное рабочее место для слабовидящих и незрячих пользователей с читающей машиной ЭлСис 207 CN; Аппаратный комплекс с функцией видеоувеличения и чтения для слабовидящих и незрячих пользователей ЭлСис 207 OS.	143907, Московская область, г. Балашиха, ул. шоссе Энтузиастов, д. 50, каб. 105 Площадь помещения 52,8 кв. м. № по технической инвентаризации 116, этаж 1

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
МИНИСТЕРСТВА СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА ИМЕНИ В.И. ВЕРНАДСКОГО»
(Университет Вернадского)

Кафедра Цифровых систем и инженерных технологий

Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Информационная безопасность

Направление подготовки 09.04.03 Прикладная информатика

Направленность (профиль) программы Искусственный интеллект и программирование

Квалификация Магистр

Форма обучения **очная**

Балашиха 2024 г.

1.Описание показателей и критериев оценивания планируемых результатов обучения по учебной дисциплине

Компетенций	Индикатор сформированности компетенций	Уровень освоения	Планируемые результаты обучения
ПК-1 Способен выполнять теоретические исследования процессов создания, накопления и обработки информации, включая анализ и создание моделей данных и знаний, языков их описания и манипулирования, разработку новых математических методов и средств поддержки интеллектуальной обработки данных	**Знать (З):** основные понятия, виды моделей, современный инструментарий и методы имитационного моделирования, проведение имитационного эксперимента; методы формализации и постановки задач имитационного моделирования **Уметь (У):** Использовать информационные технологии имитационного моделирования с использованием современных систем имитационного моделирования; методы разработки математического и программного обеспечения имитационных моделей; современные инструментарий имитационного моделирования **Владеть (В):** Построением процессов и событийных моделей дискретных систем; выполнением формализации и постановки задач имитационного моделирования; разработкой имитационных моделей систем и процессов, планированием и выполнением имитационного эксперимента с использованием систем имитационного моделирования	**Пороговый (удовлетворительно)**	**Знать:** основные понятия, виды моделей, современный инструментарий и методы имитационного моделирования, проведение имитационного эксперимента; методы формализации и постановки задач имитационного моделирования **Уметь:** Использовать информационные технологии имитационного моделирования с использованием современных систем имитационного моделирования; методы разработки математического и программного обеспечения имитационных моделей; современные инструментарий имитационного моделирования **Владеть:** Построением процессов и событийных моделей дискретных систем; выполнением формализации и постановки задач имитационного моделирования; разработкой имитационных моделей систем и процессов, планированием и выполнением имитационного эксперимента с использованием систем имитационного моделирования
		Продвинутый (хорошо)	**Знать:** основные понятия, виды моделей, современный инструментарий и методы имитационного моделирования, проведение имитационного эксперимента; методы формализации и постановки задач имитационного моделирования **Уметь:** Использовать информационные технологии имитационного моделирования с использованием современных систем имитационного моделирования; методы разработки математического и программного обеспечения имитационных моделей; современные инструментарий имитационного моделирования **Владеть:** Построением процессов и событийных моделей дискретных систем; выполнением формализации и постановки задач имитационного моделирования; разработкой имитационных моделей систем и процессов, планированием и выполнением имитационного эксперимента с использованием систем имитационного моделирования
		Высокий (отлично)	**Знать:** основные понятия, виды моделей, современный инструментарий и методы имитационного моделирования, проведение имитационного эксперимента; методы формализации и постановки задач имитационного моделирования **Уметь:** Использовать информационные технологии имитационного моделирования с использованием современных систем имитационного мо-

			делирования; методы разработки математического и программного обеспечения имитационных моделей; современные инструментарий имитационного моделирования **Владеть:** Построением процессов и событийных моделей дискретных систем; выполнением формализации и постановки задач имитационного моделирования; разработкой имитационных моделей систем и процессов, планированием и выполнением имитационного эксперимента с использованием систем имитационного моделирования
ПК-2 Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения	**Знать (З):** современные методы разработки и реализации алгоритмов математических моделей на базе языков и пакетов прикладных программ моделирования **Уметь (У):** Разработкой и реализацией алгоритмов математических моделей на базе языков и пакетов прикладных программ моделирования **Владеть (В):** в практической деятельности разработкой алгоритмов на базе языков и пакетов прикладных программ моделирования	**Пороговый (удовлетворительно)**	**Знать:** современные методы разработки и реализации алгоритмов математических моделей на базе языков и пакетов прикладных программ моделирования **Уметь:** Разработкой и реализацией алгоритмов математических моделей на базе языков и пакетов прикладных программ моделирования современные методы разработки и реализации алгоритмов математических моделей на базе языков и пакетов прикладных программ моделирования **Владеть:** в практической деятельности разработкой алгоритмов на базе языков и пакетов прикладных программ моделирования
		Продвинутый (хорошо)	**Знать:** современные методы разработки и реализации алгоритмов математических моделей на базе языков и пакетов прикладных программ моделирования **Уметь:** Разработкой и реализацией алгоритмов математических моделей на базе языков и пакетов прикладных программ моделирования **Владеть:** в практической деятельности разработкой алгоритмов на базе языков и пакетов прикладных программ моделирования
		Высокий (отлично)	**Знать:** современные методы разработки и реализации алгоритмов математических моделей на базе языков и пакетов прикладных программ моделирования **Уметь:** Разработкой и реализацией алгоритмов математических моделей на базе языков и пакетов прикладных программ моделирования **Владеть:** в практической деятельности разработкой алгоритмов на базе языков и пакетов прикладных программ моделирования

2. Описание шкал оценивания

2.1 Шкала оценивания на этапе текущего контроля

Форма текущего контроля	Отсутствие усвоения (ниже порогового)*	Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
Доклад	не выполнена или все задания решены неправильно	Цель и задачи доклада достигнуты частично. Актуальность темы определена неубедительно. В докладе выявлены значительные отклонения от требований методических указаний.	Цель и задачи выполнения доклада достигнуты. Актуальность темы подтверждена. Доклад выполнен с незначительными отклонениями от требований методических указаний.	Цель написания доклада достигнута, задачи решены. Актуальность темы исследования корректно и полно обоснована. Доклад выполнен согласно требованиям.

2.2 Шкала оценивания на этапе промежуточной аттестации (зачет и экзамен, курсовая работа)

Форма промежуточной аттестации	Отсутствие усвоения (ниже порогового)	Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
Ответы на вопросы к экзамену	не выполнена или все задания решены неправильно	Цель и задачи вопроса достигнуты частично. Актуальность темы определена неубедительно.	Цель и задачи выполнения вопроса достигнуты. Актуальность темы подтверждена.	Цель написания ответа на вопрос достигнута, задачи решены.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

ПРИМЕРНЫЕ ТЕСТОВЫЕ ЗАДАНИЯ ПО ДИСЦИПЛИНЕ

Правильный вариант ответа отмечен знаком +

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг -компании
- Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:
+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности
11) Принципом политики информационной безопасности является принцип:
+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях
12) Принципом политики информационной безопасности является принцип:
+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы
13) Принципом политики информационной безопасности является принцип:
+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы
14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания
15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его
16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа
17) ЭЦП – это:
- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
- Электронно-цифровой процессор
18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов
19) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных
20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии
21) Утечкой информации в системе называется ситуация, характеризуемая:
+ Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
+ Целостность
- Доступность
- Актуальность
23) Угроза информационной системе (компьютерной сети) – это:
+ Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически
24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- Регламентированной
- Правовой
+ Защищаемой
25) Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:
+ Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные
26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
+ Владелец сети
- Администратор сети
- Пользователь сети
27) Политика безопасности в системе (сети) – это комплекс:
+ Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети
28) Наиболее важным при реализации защитных мер политики безопасности является:
- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
+ Аудит, анализ уязвимостей, риск-ситуаций

ПРИМЕРНАЯ ТЕМАТИКА ДОКЛАДОВ

1. Развитие тестирования в рамках педологии.
2. Развитие тестирования в России.
3. Рейтинг как современное средство оценивания учебных достижений обучающихся.
4. Современное развитие тестологии.
5. Современные подходы к понятию качества образования.
6. Социально-этические аспекты тестирования.
7. Таксономия образовательных целей и результаты образования.
8. Организация самостоятельной работы обучающихся в информационной образовательной среде.
9. Учебно-методическое обеспечение для организации самостоятельной работы в условиях использования информационной образовательной среды.
10. Информационно-образовательная среда в формировании субкультуры студентов;
11. Развитие информационно-правовой культуры студентов в информационно-образовательной среде;
12. Программно-аппаратные платформы для информационных ресурсов сферы образования.

13. Понятие сетевого взаимодействия в трудах отечественных учёных;
14. Роль сетевых технологий в реализации программы информатизации высшего образования;
15. Проблемы развития технологий сетевого взаимодействия в образовании;
16. Сетевое взаимодействие в инклюзивном образовании.

ВЫПОЛНЕНИЕ КУРСОВОЙ РАБОТЫ

Выполнение курсовой работы	не показал умение собирать и систематизировать информацию из теоретических источников, анализировать практический материал, не овладел методикой исследования, не проявил творческий подход и самостоятельность в анализе, обобщениях и выводах, не аргументировал предложения, не соблюдал все требования к оформлению курсовой работы и сроков ее исполнения.	показал умение собирать информацию из теоретических источников, анализировать практический материал для иллюстраций теоретических положений, недостаточно овладел методикой исследования, не проявил творческий подход и самостоятельность в анализе, обобщениях и выводах, не аргументировал предложения, не соблюдал все требования к оформлению курсовой работы и сроков ее исполнения.	показал умение собирать и систематизировать информацию из теоретических источников, анализировать и грамотно использовать практический материал для иллюстраций теоретических положений, проявил творческий подход и самостоятельность в анализе, недостаточно аргументировал выводы и предложения, не соблюдал все требования к оформлению курсовой работы и сроков ее исполнения.	показал умение собирать и систематизировать информацию из теоретических источников, анализировать и грамотно использовать практический материал для иллюстраций теоретических положений, проявил творческий подход и самостоятельность в анализе, обобщениях и выводах, аргументировал предложения, соблюдал все требования к оформлению курсовой работы и сроков ее исполнения.

ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ РАБОТ

1. Информация - фактор существования и развития общества. Основные формы проявления информации, её свойства как объекта безопасности.
2. Понятие безопасности и её составляющие. Безопасность информации.
3. Обеспечение информационной безопасности: содержание и структура понятия.
4. Национальные интересы в информационной сфере.
5. Источники и содержание угроз в информационной сфере.
6. Соотношение понятий «информационная безопасность» и «национальная безопасность»
7. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.
8. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.
9. Система обеспечения информационной безопасности.
10. Обеспечение информационной безопасности Российской Федерации.
11. Понятие информационной войны. Проблемы информационной войны.
12. Информационное оружие и его классификация.
13. Цели информационной войны, её составные части и средства её ведения. Объекты воздействия в информационной войне.
14. Уровни ведения информационной войны. Информационные операции. Психологические операции.
15. Уровни ведения информационной войны. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.
16. Основные положения государственной информационной политики Российской

Федерации.
17. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.
18. Виды защищаемой информации в сфере государственного и муниципального управления.
19. Обеспечение информационной безопасности организации.
20. Характеристика эффективных стандартов по безопасности.
21. Требования к полноте эффективных стандартов по безопасности.
22. Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.
23. Информация - фактор существования и развития общества.
24. Обеспечение информационной безопасности: содержание и структура понятия.
25. Система обеспечения информационной безопасности. Обеспечение информационной безопасности организации.
26. Обеспечение информационной безопасности Российской Федерации.
27. Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности
28. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.
29. Административный уровень обеспечения информационной безопасности.
30. Организационные структуры системы обеспечения информационной безопасности предприятия (организации).
31. Корпоративная нормативная база по защите информации.
32. Основные организационные мероприятия по обеспечению информационной безопасности организации (предприятия).
33. Основные организационные мероприятия по обеспечению информационной безопасности организации (предприятия).
34. Нормативно-методические документы по обеспечению безопасности информации.
35. Управление персоналом на предприятиях и в организациях.
36. Подбор и расстановка кадров.
37. Мотивация добросовестной деятельности сотрудников.
38. Порядок проведения служебных расследований.
39. Организация подготовки кадров и повышения квалификации в области обеспечения информационной безопасности.
40. Категорирование объектов информатизации.
41. Общие положения по категорированию объектов информатизации. Порядок проведения категорирования объектов на предприятий.
42. Классификация автоматизированных систем в составе объектов вычислительной техники.
43. Правовые основы лицензирования. Основные понятия и принципы лицензирования. Общие положения по организации лицензирования.
44. Государственная система лицензирования. Система лицензирования деятельности в области защиты государственной тайны.
45. Правовые основы сертификации и аттестации средств защиты информации.
46. Основные понятия и принципы сертификации.
47. Организация и проведение сертификации.
48. Организация и проведение лицензирования, сертификации и аттестации.
49. Требования к объектам информатизации и необходимость проведения их аттестации. Порядок проведения аттестации объектов информатизации.
50. Права и обязанности органов системы аттестации объектов информатизации.
51. Проведение аттестационных испытаний.
52. Основы организации и обеспечения работ по технической защите информации.

53. Цели и задачи защиты информации.
54. Организация защиты конфиденциальной информации.
55. Концепция безопасности предприятия и ее содержание.
56. Организация работы подразделений (служб) обеспечения информационной безопасности.
57. Организация защиты информации на предприятии.
58. Выявление и классификация угроз.
59. Принципы обеспечения информационной безопасности.
60. Управление информационной безопасностью.
61. Политика безопасности.
62. Разработка и внедрение системы управления информационной безопасности. Обеспечение информационной безопасности организации.
63. Характеристика эффективных стандартов по безопасности.
64. Требования к полноте эффективных стандартов по безопасности.
65. Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.
66. Информация - фактор существования и развития общества.
67. Обеспечение информационной безопасности: содержание и структура понятия.
68. Система обеспечения информационной безопасности. Обеспечение информационной безопасности организации.
69. Обеспечение информационной безопасности Российской Федерации.
70. Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности
71. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.
72. Административный уровень обеспечения информационной безопасности.
73. Общие положения по категорированию объектов информатизации. Порядок проведения категорирования объектов на предприятий.
74. Классификация автоматизированных систем в составе объектов вычислительной техники.
75. Правовые основы лицензирования. Основные понятия и принципы лицензирования. Общие положения по организации лицензирования.
76. Государственная система лицензирования. Система лицензирования деятельности в области защиты государственной тайны.
77. Правовые основы сертификации и аттестации средств защиты информации.
78. Основные понятия и принципы сертификации.
79. Организация и проведение сертификации.
80. Организация и проведение лицензирования, сертификации и аттестации.
81. Уровни ведения информационной войны. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.
82. Основные положения государственной информационной политики Российской Федерации.
83. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.
84. Виды защищаемой информации в сфере государственного и муниципального управления.
85. Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности
86. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.
87. Административный уровень обеспечения информационной безопасности.

ПРИМЕРНАЯ ТЕМАТИКА ВОПРОСОВ К ЭКЗАМЕНУ

1. Роль информации в современном мире. Понятие о защищаемой информации.
2. Теория информационной безопасности. Основные направления.
3. Обеспечение ИБ и направления защиты.
4. Требования к системе и политике ИБ.
5. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
6. Доктрина информационной безопасности РФ.
7. Защита государственной тайны в РФ.
8. Защита коммерческой тайны в РФ.
9. Защита персональных данных в РФ.
10. Защита служебной и профессиональной тайны в РФ.
11. Процедуры сертификации и аттестации в РФ.
12. Понятие о защищаемой информации. Свойства информации.
13. Угрозы информации. Классификация угроз.
14. Угрозы нарушения конфиденциальности информации. Особенности и примеры реализации угроз.
15. Угрозы нарушения целостности информации. Особенности и примеры реализации угроз.
16. Угроза нарушения доступности информации. Особенности и примеры реализации угрозы.
17. Источники угроз. Классификация источников угроз.
18. Идентификация и аутентификация. Использование парольной защиты. Недостатки парольной защиты.
19. Понятие электронной подписи.
20. Организационные меры обеспечения информационной безопасности. Служба безопасности предприятия.
21. Организация внутри объектового режима предприятия. Организация охраны.
22. Криптографические меры обеспечения информационной безопасности. Классификация криптографических алгоритмов.
23. Программно-аппаратные защиты информации. Межсетевые экраны, их функции и назначения.
24. Программно-аппаратные защиты информации. Антивирусные средства, их функции и назначения.
25. Особенности защиты беспроводных и мобильных подключений.
26. Симметричное и ассиметричное шифрование.
27. Принципы симметричного шифрования.
28. Односторонние функции и их применение.
29. Простейшие методы ассиметричного шифрования.
30. Метод RSA.
31. Электронная подпись и ее применение.