МИНОБРНАУКИ РОССИИ
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**
**(ФГБОУ ВО «ВГУ»)**

**УТВЕРЖДАЮ**

Заведующий кафедрой
*функционального анализа*
*и операторных уравнений*

*Каменский М.И.*
*подпись, расшифровка подписи*
25.05.2023

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

## Б1.О.03.01 Основы информационной безопасности

**1. Код и наименование направления специальности:** 10.05.04 Информационно-аналитические системы безопасности

**2. Профиль специализация:** Автоматизация информационно-аналитической деятельности

**3. Квалификация выпускника:** специалист

**4. Форма обучения:** очная

**5. Кафедра, отвечающая за реализацию дисциплины:** функционального анализа и операторных уравнений

**6. Составители программы:** Завгородний Михаил Григорьевич, Канд. физ-мат. наук, доцент

**7**. **Рекомендована:** НМС математического факультета, протокол №0500-06 от 25.05.2023 г.

**8. Учебный год:** 2023-2024 **Семестр(ы):** 2

**9**.**Цели и задачи учебной дисциплины:** Цель курса – дать необходимые понятия информационной безопасности и заложить терминологический фундамент; рассмотреть основные общеметодологические принципы теории информационной безопасности; научить правомерно анализировать угрозы безопасности информации, определять источники этих угроз, способы реализации и цели угроз информационной безопасности; изучение методов и средств обеспечения информационной безопасности, методов защиты информации от нарушения ее конфиденциальности, целостности и доступности информации; выполнять основные этапы решения задач информационной безопасности.

Основными задачами изучения дисциплины являются:

- ознакомление студентов с понятиями и терминологией информационной безопасности;
- усвоение знаний по нормативно-правовым основам организации информационной безопасности;
- изучение характеристик основных угроз информационной безопасности, каналов утечки информации и методов компьютерного шпионажа;
- получение представлений о существующих правовых, организационных методах и технических средствах защиты информации от несанкционированного доступа и от модификации и удаления;
- освоение критериев эффективности мер по защите информации.

**10. Место учебной дисциплины в структуре ООП:**

Дисциплина входит в базовую (общепрофессиональную) часть профессионального цикла. Для изучения и освоения дисциплины нужны знания из предшествующих курсов: Правоведение, Дискретная математика, Информатика, Математическая логика и теория алгоритмов, Языки программирования, Технология и методы программирования. Знания и умения, приобретенные студентами в результате изучения дисциплины, будут использоваться при изучении курсов: Безопасность операционных систем, Безопасность электронного документооборота, Криптографические методы защиты информации, Безопасность информационных и аналитических систем, Моделирование автоматизированных информационных систем, Принципы построения, проектирования и эксплуатации автоматизированных информационных систем, Безопасность сетей ЭВМ, Безопасность программного обеспечения, а также при выполнении курсовых и дипломных работ, связанных с математическим моделированием в области информационной безопасности и защиты информации.

**11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):**

| Код | Название компетенции | Код(ы) | Индикатор(ы) | Планируемые результаты обучения |
|---|---|---|---|---|
| ОПК-1 | Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их | ОПК-1.2 | Способен оценивать роль информационной безопасности в современном обществе, ее значение для обеспечения объективных | **знать:**<br>основы информационной безопасности<br>основные понятия по информационной безопасности,<br>требования, предъявляемые к системе защиты современных ОС;<br>**уметь:**<br>оценивать роль информации, информационных технологий и информационной безопасности в |

| | | | | |
|---|---|---|---|---|
| | значение для обеспечения объективных потребностей личности, общества и государства; | | потребностей личности, общества и государства | современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;<br>применять аппарат нечеткой логики, математической логики и теории алгоритмов для формализации предметной области;<br>**владеть:**<br>методами и средствами информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства. |

## 12. Объем дисциплины в зачетных единицах/час — 3/108.

**Форма промежуточной аттестации:** зачет

## 13. Виды учебной работы

| Вид учебной работы | | Трудоемкость | |
|---|---|---|---|
| | | Всего | По семестрам |
| | | | 2 семестр |
| Аудиторные занятия | | 50 | 50 |
| в том числе: | лекции | 34 | 34 |
| | практические | 16 | 16 |
| | лабораторные | | |
| Самостоятельная работа | | 58 | 58 |
| Форма промежуточной аттестации *(экзамен – __час.)* | | | |
| Итого: | | 108 | 108 |

### 13.1. Содержание дисциплины

| № п/п | Наименование раздела дисциплины | Содержание раздела дисциплины |
|---|---|---|
| 1 | Введение в теорию информационной безопасности | Основные понятия и определения. Концептуальные основы информационной безопасности и защиты информации |
| 2 | Структура информационных ресурсов. Интеллектуальная собственность и коммерческая тайна. | Понятие об информационных ресурсах. Понятия интеллектуальной собственности и коммерческой тайны, их структура. Персональные данные. Принципы информационной безопасности. |
| 3 | Угрозы информационной безопасности и их классификация. | Угрозы информационным ресурсам: угрозы несанкционированного доступа, модификации и удаления информации; угрозы криминогенного характера, природного и техногенного характера, угрозы, связанные с неквалифицированным пользованием информационными ресурсами. Компьютерный шпионаж, его цели и методы. Внутренние и внешние факторы, способствующие компьютерному шпионажу. Характеристика каналов утечки информации. Активный и пассивный доступ к информационным ресурсам. |
| 4 | Правовые аспекты защиты информации. | Понятие о правовых средствах защиты информации. Законы, регулирующие деятельность по защите |

| | | |
|---|---|---|
| | | информации. Охрана объектов интеллектуальной собственности. Проблемы, возникающие при реализации правовых мер защиты информации. |
| 5 | Организационные мероприятия, направленные на защиту информации. | Ограничение и разграничение доступа к информации. Дублирование важной информации на разнотипных носителях. Многоуровневая система защиты информации. |
| 6 | Программно-аппаратные средства защиты информации | Пароли и системы с многоуровневым доступом. «Защита от дурака» в компьютерных программах. Защита программ и электронных баз данных. Антивирусные программы. Защита каналов связи. Повреждение информации в каналах связи и средства борьбы с ним. |
| 7 | Математические методы и модели в задачах защиты информации. | Методы сжатия информации. Криптографические методы защиты информации. Шифрование с симметричными и ассимметричными ключами. |
| 8 | Эффективность мероприятий по защите информации | Частный функциональный критерий информационной безопасности и его формула для мероприятий по предотвращению несанкционированного доступа. Структура понесенного и предотвращенного ущерба от несанкционированного доступа к информации. Структура затрат на защиту информации. |

## 13.2. Темы (разделы) дисциплины и виды занятий

| № п/п | Наименование раздела дисциплины | Виды занятий (часов) | | | | |
|---|---|---|---|---|---|---|
| | | Лекции | Лабораторные | Самостоятельная работа | Контроль | Всего |
| 1 | Введение в теорию информационной безопасности | 2 | 2 | 2 | 4 | 10 |
| 2 | Структура информационных ресурсов. Интеллектуальная собственность и коммерческая тайна. | 4 | 2 | 4 | 5 | 15 |
| 3 | Угрозы информационной безопасности и их классификация. | 6 | 2 | 2 | 4 | 14 |
| 4 | Правовые аспекты защиты информации. | 2 | 2 | 4 | 5 | 13 |
| 5 | Организационные мероприятия, направленные на защиту информации. | 4 | 2 | 2 | 4 | 12 |
| 6 | Программно-аппаратные средства защиты информации | 6 | 2 | 4 | 5 | 17 |
| 7 | Математические методы и модели в задачах защиты информации. | 6 | 2 | 2 | 4 | 14 |
| 8 | Эффективность мероприятий по защите информации | 4 | 2 | 2 | 5 | 13 |
| | | | | | | |
| | Итого | 34 | 16 | 22 | 36 | 108 |

## 14. Методические указания для обучающихся по освоению дисциплины

*(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)*

## 15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины *(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*

| № п/п | Источник |
|---|---|
| *1* | *Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное* |

| | |
|---|---|
| | *пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил .— (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.* |
| | |
| *2* | *Чубукова, Светлана Георгиевна. Основы правовой информатики (юридические и математические вопросы информатики) : учебное пособие для студ. / С.Г. Чубукова, В.Д. Элькин ; Моск. гос. юрид. акад.; под ред. М.М. Рассолова .— М. : Контракт, 2004 .— 247 с. : ил. — На обл. авт. не указан .— Библиогр. в конце глав .— ISBN 5-900785-84-X.программирование / А.В. Аграновский, Р.А. Хади .— М. : СОЛОН-Пресс, 2002 .— 254, [1] с. : ил.* |
| | |
| *3* | *Иванов, Михаил Александрович. Криптографические методы защиты информации в компьютерных системах и сетях / Иванов М. А. — М. : Кудиц-Образ, 2001 .— 363 с. : ил.* |
| | |
| *4* | *Астанин, Иван Константинович. Защита информации : учебное пособие для вузов / И.К. Астанин, Н.И. Астанин ; Воронеж. гос. ун-т, Лискинский филиал .— Воронеж : Воронеж. гос. ун-т, 2006 .— Библиогр. : с.169 .— ISBN 5-9273-1080-x.* |
| | |

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

**16. Перечень учебно-методического обеспечения для самостоятельной работы** *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)*

| № п/п | Источник |
|---|---|
| *5* | *Скоромников, Кир Серафимович. Компьютерное право Российской Федерации : Учебник / К.С.Скоромников;Междунар.независим. эколого-политол.ун-т .— М. : Изд-во МНЭПУ, 2000 .— 220,[1] с. — ISBN 5-7383-0105-6.* |
| | |
| *6* | *Велпури, Рама. Oracle8i : Резервное копирование и восстановление / Р. Велпури, А. Адколи ; Пер.с англ. И. Афанасьева; Науч. ред. А. Головко; Авт. предислов. Я. Текер .— М. : Лори, 2002 .— 572 с. : ил .— Парал. тит. л. англ. — ISBN 5-85582-166-8.* |
| | |
| *7* | *Гайдамакин, Н.А. Разграничение доступа к информации в компьютерных системах / Н.А. Гайдамакин .— Екатеринбург : Изд-во Уральского ун-та, 2003 .— 327 с. : ил .— Библиогр.:с.317-322 .— Алф.-предм. указ.: с.306-316 .— ISBN 5-86037-024-5.* |
| | |
| *8* | *Голуб, Владимир Александрович. Информационная безопасность телекоммуникационных систем : Учебное пособие .— Воронеж : Студия ИАН, 2002 .— 157,[1] с. — ISBN 5-86026-020-2 : 37.00 .— <URL:http://www.lib.vsu.ru/elib/books/b102829.djvu>.* |

**17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):**

Дисциплина может реализовываться с применением электронного обучения и дистанционных образовательных технологий. При проведении занятий в дистанционной форме используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ" (https://edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете, а также другие доступные ресурсы в сети Интернет.

---

**18. Материально-техническое обеспечение дисциплины:**

---

Для проведения лекционных и лабораторных занятий используются аудитории, соответствующие действующим санитарно-техническим нормам и противопожарным правилам.
Для проведения лабораторных занятий и самостоятельной работы используется класс с компьютерной техникой, оснащенный необходимым программным обеспечением, электронными учебными пособиями и законодательно - правовой и нормативной поисковой системой, имеющий выход в глобальную сеть.

## 19. Оценочные средства для проведения текущей и промежуточной аттестаций:

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

| № п/п | Наименование раздела дисциплины | Компетенция(и) | Индикатор(ы) достижения компетенции | Оценочные средства |
|---|---|---|---|---|
| 1 | Введение в теорию информационной безопасности | ОПК-1 | ОПК-1.2 | Домашнее задание, контрольная работа |
| 2 | Структура информационных ресурсов. Интеллектуальная собственность и коммерческая тайна. | ОПК-1 | ОПК-1.2 | Домашнее задание, контрольная работа |
| 3 | Угрозы информационной безопасности и их классификация. | ОПК-1 | ОПК-1.2 | Домашнее задание, контрольная работа |
| 4 | Правовые аспекты защиты информации. | ОПК-1 | ОПК-1.2 | Домашнее задание, контрольная работа |
| 5 | Организационные мероприятия, направленные на защиту информации. | ОПК-1 | ОПК-1.2 | Домашнее задание, контрольная работа |
| 6 | Программно-аппаратные средства защиты информации | ОПК-1 | ОПК-1.2 | Домашнее задание, контрольная работа |
| 7 | Математические методы и модели в задачах защиты информации. | ОПК-1 | ОПК-1.2 | Домашнее задание, контрольная работа |
| 8 | Эффективность мероприятий по защите информации | ОПК-1 | ОПК-1.2 | Домашнее задание, контрольная работа |
| | Промежуточная аттестация форма контроля – зачёт | | | Перечень вопросов Практическое задание |

## 20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

### 20.1 Текущий контроль успеваемости

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в форме лабораторных работ и контрольной работы.

При оценивании используется следующая шкала:

5 баллов ставится, если обучающийся демонстрирует полное соответствие знаний, умений, навыков приведенным в таблицах показателям, свободно оперирует приобретенными знаниями, умениями, применяет их при решении практических задач;

4 балла ставится, если обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач;

3 балла ставится, если обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач;

2 балла ставится, если обучающийся демонстрирует явное несоответствие знаний, умений, навыков приведенным в таблицах показателям.

*При сдаче экзамена*
оценка «отлично» - 5 баллов
оценка «хорошо» - 4 балла
оценка «удовлетворительно» - 3 балла
оценка «неудовлетворительно» - 2 балла.

| Критерии оценивания компетенций | Уровень сформированности компетенций | Шкала оценок |
|---|---|---|
| *Обучающийся в полной мере владеет понятийным аппаратом в области программирования и технологии работы на ЭВМ, способен иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач программирования, СУБД и сетевых технологий.* | *Повышенный уровень* | *Отлично* |
| *У обучающегося сформированы знания, умения и навыки программирования и технологии работы на ЭВМ; он способен иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач; но допускает отдельные несущественные пробелы в своих знаниях, допускает ошибки при выполнении практических задач.* | *Базовый уровень* | *Хорошо* |
| *У обучающегося сформированы неполные знания, умения и навыки; он допускает отдельные существенные пробелы в своих знаниях, допускает существенные ошибки при выполнении практических задач.* | *Пороговый уровень* | *Удовлетвори-тельно* |
| *Сформированы лишь фрагментарные знания, умения и навыки или знания, умения и навыки отсутствуют* | – | *Неудовлетвори-тельно* |

**20.2 Промежуточная аттестация**

**Пример лабораторного задания (вариант задания)**

Лабораторная работа № ___

по дисциплине «Основы информационной безопасности»

Тема: «**Шифрование с открытым ключом методом укладки рюкзака**»

***Задание.*** Выберите текст (не менее 60 символов) для шифрования методом укладки рюкзака. Сформируйте закрытую и открытую части ключа. При этом учтите требования, предъявляемые к выбору ключа с целью повышения криптостойкости. Зашифруйте выбранный текст. Сформируйте шифрграмму.

Обменяйтесь шифрграммами. Расшифруйте полученный шифртекст. Предполагается, что Вы знаете закрытую и открытую части ключа. Подготовьте отчет.

### *Вопросы*

1. Какие криптосистемы относятся к системам шифрования с открытым ключом? В чем их особенность?
2. Сформулируйте математические основы шифрования с открытым ключом
3. Сформулируйте математические основы шифрования методом укладки рюкзака.

По результатам выполнения заданий подготовьте отчет.

***Отчет по лабораторной работе № должен содержать:***

1) Титульный лист.
2) Выбранный текст для шифрования.
3) Пояснения по выбору ключа с поверкой требований, предъявляемых к выбору ключа.
4) Пояснения по шифрованию и полученный шифртекст.
5) Шифрграмму, подготовленную Вами, с указанием открытой части ключа.
6) Шифрграмму, полученную Вами при обмене.
7) Пояснения по расшифрованию и полученный открытый текст.
8) Ответы на вопросы.
9) Ваши выводы.

### Пример контрольного задания (вариант задания)

Контрольная работа
по дисциплине «Основы информационной безопасности»
Вариант №___

В результате шифрования методом Вижинера был получен следующий шифртекст: «СПЦСЗЗЮУГИВЕБЬБТЖЩИОБ». Прочитайте этот шифртекст, если известно, что шифрующая последовательность содержит только символы А, Б и В.

### Примерный перечень вопросов к экзамену

1. Правовое регулирование в области безопасности информации: законодательная база информатизации общества; структура государственных органов, обеспечивающих безопасность информационных технологий.
2. Информационная безопасность. Основные определения.
3. Угрозы информационной безопасности.
4. Модель системы зашиты.
5. Организационные меры и меры обеспечения физической безопасности.
6. Идентификация и аутентификация. Методы аутентификации.

7. Особенности парольных систем аутентификации: рекомендации по практической реализации парольных систем, оценка стойкости парольных систем, методы хранения паролей.

8. Методы разграничения доступа. Криптографические методы обеспечения конфиденциальности информации.

9. Методы зашиты внешнего периметра.

10. Системы обнаружения вторжений (Intrusion Detection System, EDS).

11. Протоколирование и аудит.

12. Построение систем защиты от угроз нарушения целостности: типовая структура такой системы.

13. Криптографические методы обеспечения целостности информации: реализация механизма цифровой подписи, криптографические хэш-функции и ее преимущества, коды проверки подлинности.

14. Структура системы защиты от угроз нарушения доступности: поясните основные составляющие.

15. Формальные модели управления доступом: модель Харрисона-Руззо-Ульмана, модель Беллл-ЛаПалулы.

16. Формальные модели целостности: модель Кларка-Вилсона, модель Биба.

17. Основные положения ISO/IEC 15408. Критерии оценки безопасности информационных технологий. Понятия безопасности и их взаимосвязь в соответствии с ГОСТ Р ИСО/МЭК 15408-2002. Структура профиля защиты в соответствии с ГОСТ Р ИСО/МЭК 15408-2002.

18 Основные положения ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. Практические правила управления информационной безопасностью".

19 Основные положения ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования". Этапы построения и использования СМИБ.

20 Обобщенная схема построения комплексной защиты компьютерной сети предприятия на примере модели Lifecycle Security.

21 Технология функционирования VPN. Типы виртуальных частных сетей, преимущества и недостатки.

22 Методика анализа рисков в сфере информационной безопасности CRAMM.

23 Методика анализа рисков в сфере информационной безопасности FRAP.

24 Методика анализа рисков в сфере информационной безопасности OCTAVE.

25 Методика анализа рисков в сфере информационной безопасности RiskWatch.

26 Проведение оценки рисков в соответствии с методикой Microsoft.

27 Опишите суть протокола системы централизованной аутентификации и распределе-ния ключей симметричного шифрования Kerberos Протоколы и механизмы обеспечения информационной безопасности Kerberos, S/MIME, IPSec, AH, ESP, IPSec, NAT. Опишите их назначение и область применения.

## Пример контрольно-измерительного материала

**Б ВГУ 038.824-2016**
УТВЕРЖДАЮ
заведующий кафедрой функционального анализа и операторных уравнений
М.И. Каменский
*подпись, расшифровка подписи*

Направление подготовки / специальность: 10.05.04 Информационно-аналитические системы безопасности
*шифр, наименование*
Дисциплина Основы информационной безопасности
Вид контроля экзамен
*промежуточный контроль - экзамен, зачет; текущий контроль с указанием формы*

Контрольно-измерительный материал №___

1. Угрозы информационной безопасности.

2. Методика анализа рисков в сфере информационной безопасности OCTAVE.

Преподаватель _____ _____
*подпись расшифровка подписи*