Министерство сельского хозяйства Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Горский государственный аграрный университет»
(ФГБОУ ВО Горский ГАУ)

Факультет Межфакультетский центр

Кафедра Информационных технологий

Учебный год 2024-2025

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

## ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ОБРАЗОВАНИЯ -

## ПРОГРАММА СПЕЦИАЛИТЕТА

| | |
|---|---|
| Наименование направления подготовки | 38.05.01 Экономическая безопасность |
| Направленность (профиль) | Экономико-правовое обеспечение экономической безопасности |
| Реквизиты федерального государственного образовательного стандарта высшего образования | Приказ Минобрнауки России от 14 апреля 2021 г. № 293 |
| Год начала подготовки | 2022 |
| Очная форма обучения - учебные планы по годам приема | 2023,2024 |
| Заочная форма обучения - учебные планы по годам приема | 2022,2023,2024 |
| Номер по реестру ОП ВО ФГБОУ ВО Горский ГАУ | С-380501-2022 |
| Реквизиты решения ученого совета ФГБОУ ВО Горский ГАУ об утверждении ОП ВО | Протокол от 19 января 2024 г. № 3 |
| Реквизиты приказа ректора или уполномоченного лица об утверждении ОП ВО | Приказ ректора от 29 февраля 2024 г. № 52/06 |
| Место дисциплины в структуре учебного плана | Обязательная часть |
| Количество зачетных единиц | 3 ЗЕ |

ВЛАДИКАВКАЗ – 2024

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

| № № | Планируемые результаты освоения образовательной программы | | Код и наименование индикатора достижения компетенции | Планируемые результаты обучения по дисциплине | Направление воспитательной работы |
|---|---|---|---|---|---|
| | Наименование категории (группы) компетенций | Код и наименование компетенции | | | |
| | | ОПК-6 Способен использовать современные информационные технологии и программные средства при решении профессиональных задач | ОПК-6. И-1. Понимает базовые принципы использования современных информационных технологий и программных средств | Знает базовые принципы использования современных информационных технологий и программных средств. | |
| | | | | Умеет анализировать профессиональные задачи, выбирать и использовать подходящие ИТ-решения. | |
| | | | | Владеет современными программно-техническими платформами и программными средствами, в том числе отечественного производства, способен анализировать профессиональные задачи, выбирая и используя подходящие ИТ-решения. | |
| | | | ОПК-6. И-2. Применяет современные информационные технологии и программные средства для решения профессиональных задач. | Знает специализированные пакеты прикладных программ, предназначенные для решения профессиональных задач. | |
| | | | | Умеет использовать современные информационные технологии и программные средства для решения профессиональных задач. | |
| | | | | Владеет навыками анализа профессиональных задач и способен применять современных программно-технические платформы и программные средства, в том числе отечественного производства в профессиональной деятельности. | |

Принятые далее сокращения по тексту:
Л – лекционное занятие;
ПЗ – практическое занятие;
ЛР – лабораторная работа;
СРС – самостоятельная работа студентов.

## 2. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ

2.1. Трудоемкость дисциплины по видам учебной деятельности и формам обучения:

| Виды учебной деятельности | Всего часов 108ч, в том числе часов: | | |
|---|---|---|---|
| | Очная форма обучения | Заочная форма обучения | Очно-заочная форма обучения |
| Лекционные занятия | 18 | 4 | – |
| Практические (лабораторные, др.) занятия | 24 | 6 | – |
| Самостоятельная работа | 66 | 98 | – |
| Форма промежуточной аттестации | Зачёт | | |

2.2. Трудоемкость дисциплины по (разделам) темам:

| № № п/п | Наименование тем | Всего часов | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Очная форма обучения | | | Заочная форма обучения | | | Очно-заочная форма обучения | | |
| | | Лекции | Практические (лабораторные, др.) занятия | СРС | Лекции | Практические (лабораторные, др.) занятия | СРС | Лекции | Практические (лабораторные, др.) занятия | СРС |
| 1. | Тема 1. Основные понятия теории информационной безопасности. | 2 | 2 | 8 | 2 | 2 | 12 | – | – | – |
| 2. | Тема 2. Информация как объект защиты. | 2 | 2 | 8 | | | 12 | – | – | – |
| 3. | Тема 3. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности. Угрозы информационной безопасности. | 4 | 4 | 10 | | | 14 | – | – | – |
| 4. | Тема 4. Построение систем защиты от угрозы нарушения конфиденциальности. | 2 | 4 | 8 | | 2 | 12 | – | – | – |
| 5. | Тема 5. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа. | 2 | 2 | 8 | 2 | | 12 | – | – | – |
| 6. | Тема 6. Политика и модели безопасности. | 2 | 4 | 8 | | | 12 | – | – | – |
| 7. | Тема 7. Обзор международных стандартов информационной безопасности. | 2 | 2 | 8 | | 2 | 12 | – | – | – |
| 8. | Тема 8. Информационные войны и информационное противоборство. | 2 | 4 | 8 | | | 12 | – | – | – |

## 3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ

### ТЕМА 1. ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

На лекции рассматриваются цели и задачи учебной дисциплины. Вводятся основные понятия. История становления теории информационной безопасности. Предметная область теории информационной безопасности. Систематизация понятий в области защиты информации. Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Понятие предметной области «защита информации». Основные принципы построения систем защиты. Концепция комплексной защиты информации. Задачи защиты информации. Средства реализации комплексной защиты информации.

В РАМКАХ ДАННОЙ ТЕМЫ ПРЕДУСМОТРЕНЫ ПРАКТИЧЕСКИЕ ЗАНЯТИЯ.

Вопросы практического занятия:
ПЗ: Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации (в программе L_LUX.exe). Методы шифрования одноалфавитный метод. Шифрование методом перестановки символов. Шифрование инверсными символами (по дополнению до 255). Многоалфавитные методы шифрования. Основные требования, предъявляемые к методам шифрования текста.

ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПРЕДЛАГАЮТСЯ СЛЕДУЮЩИЕ ВОПРОСЫ:

1). Защита информации в России (периоды, факторы влияния, деятельность по защите, органы защиты).
2). Защита информации в СССР с 1917-1995 (периоды, факторы влияния, деятельность по защите, органы защиты).
3). Перспективные направления исследований в области информационной безопасности.
4). Какие методы защиты информации, использовавшиеся в древнее время и в Средние века Вам известны?
5). Покажите связь между уровнем развития общества и технологиями защиты информации.
6). В каких направлениях идет развитие теории информационной безопасности в настоящее время?
7). Каков вклад российских ученых в теорию информационной безопасности?
8). С чем связан возросший интерес к проблемам защиты информации?

### ТЕМА 2. ИНФОРМАЦИЯ КАК ОБЪЕКТ ЗАЩИТЫ.

Понятие об информации как объекте защиты. Уровни представления информации. Основные свойства защищаемой информации. Виды и формы представления информации. Информационные ресурсы.
Структура и шкала ценности информации. Классификация информационных ресурсов. Правовой режим информационных ресурсов.

В РАМКАХ ДАННОЙ ТЕМЫ ПРЕДУСМОТРЕНЫ ПРАКТИЧЕСКИЕ ЗАНЯТИЯ.

Вопросы практического занятия:
ПЗ: Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей. Изучить методы шифрования/расшифрования перестановкой символов, подстановкой, гаммированием. Использованием таблицы Виженера. Исследование и сравнение стойкости различных методов на основе атак путём перебора всех возможных ключей.

ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПРЕДЛАГАЮТСЯ СЛЕДУЮЩИЕ ВОПРОСЫ:

1). Информационные ресурсы. Классификация информационных ресурсов.
2). Что такое информация и каковы уровни ее представления?
3). Перечислите основные носители информации, особенности их использования и защиты.
4). Какими свойствами определяется ценность информации?
5). Какие критерии оценки ценности информации Вы можете предложить?

6). Приведите примеры различной зависимости ценности информации от времени.
7). Что понимается под информационными ресурсами?
8). Что не разрешается относить к информации ограниченного доступа?
9). Что понимается под конфиденциальной информацией?
10). Какие существуют виды тайны?
11). Какое назначение имеет перечень конфиденциальных сведений предприятия?

ТЕМА 3. ГОСУДАРСТВЕННАЯ ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. КОНЦЕПЦИЯ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Информационная безопасность и её место в системе национальной безопасности Российской Федерации. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.
Анализ уязвимости системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы.

В РАМКАХ ДАННОЙ ТЕМЫ ПРЕДУСМОТРЕНЫ ПРАКТИЧЕСКИЕ ЗАНЯТИЯ.

Вопросы практического занятия:
ПЗ: Изучение методов генерации простых чисел, используемых в (ассиметричных) системах шифрования с открытым ключом (в программе L_PROST.exe). Изучение функций главного меню программы (Генерация простого P, Поиск в интервале, Проверка на простоту, Вывод результатов). Проверить на простоту два произвольных целых числа разрядностью не менее 5.

ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПРЕДЛАГАЮТСЯ СЛЕДУЮЩИЕ ВОПРОСЫ:

1). Каково место информационной безопасности в системе национальной безопасности Российской Федерации?
2). Сформулируйте основные положения Доктрины информационной безопасности РФ.
3). Каковы основные цели защиты информации?
4). Каковы основные задачи в области информационной безопасности?
5). Какова структура государственной системы защиты информации?
6). Кто несет ответственность за нарушение режима защиты информации?
7). Каковы функции руководителей предприятий при организации защиты информации?
8). Покажите роль различных министерств и ведомств в вопросах защиты информации.
9). Приведите примеры систем, для которых наибольшую угрозу безопасности представляет нарушение конфиденциальности информации.
10). Для каких систем (приведите примеры) наибольшую опасность представляет нарушение целостности информации?
11). В каких системах на первом месте стоит обеспечение доступности информации?
12). В чем различие понятий «нарушение конфиденциальности информации», «несанкционированный доступ к информации», «утечка информации»?

ТЕМА 4. ПОСТРОЕНИЕ СИСТЕМ ЗАЩИТЫ ОТ УГРОЗЫ НАРУШЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ.

Определение и основные способы несанкционированного доступа (НСД). Методы защиты от НСД. Организационные методы защиты от НСД. Инженерно-технические методы защиты от НСД. Построение систем защиты от угрозы утечки по техническим каналам. Идентификация и аутентификация. Основные направления и цели использования криптографических методов. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.

В РАМКАХ ДАННОЙ ТЕМЫ ПРЕДУСМОТРЕНЫ ПРАКТИЧЕСКИЕ ЗАНЯТИЯ.

Вопросы практического занятия:
ПЗ: Ознакомление с принципами защищенного электронного документооборота в телекоммуникационных сетях и алгоритмами постановки электронной цифровой подписи (ЭЦП). Принцип по-

строения ЭЦП. Процедура постановки подписи. Процедура проверки подписи. Однонаправленные хэш-функции. Алгоритм цифровой подписи DSA. Новые стандарты ЭЦП. (на примере программы labWork6.exe)

ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПРЕДЛАГАЮТСЯ СЛЕДУЮЩИЕ ВОПРОСЫ:

1). В чем отличие терминов «Несанкционированного доступа» и «Нарушение конфиденциальности информации»?
2). Что понимается под утечкой информации?
3). Каким образом классифицируются каналы утечки информации?
4). Каким образом следует выбирать меры защиты конфиденциальности информации?
5). Дайте определение идентификации и аутентификации пользователя. В чем разница между этими понятиями?
6). Перечислите основные способы аутентификации. Какой, на ваш взгляд, является наиболее эффективным?
7). Какие основные методы контроля доступа используются в известных вам информационных системах? В чем их достоинства и недостатки?
8). Почему аутентификация с использованием пароля считается в настоящее время ненадежной?
9). Каковы методы аутентификации с использованием предметов заданного типа? Назовите те, которые получили распространение в последнее время.
10). Дайте определение шифра и сформулируйте основные требования к нему. Поясните, что понимается под совершенным шифром.
11). Почему большинство современных шифрограмм могут быть однозначно дешифрованы?
12). Каким образом государство регулирует использование средств крипозащиты?

## ТЕМА 5. ПОСТРОЕНИЕ СИСТЕМ ЗАЩИТЫ ОТ УГРОЗЫ НАРУШЕНИЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ И ОТКАЗА ДОСТУПА.

Защита целостности информации при хранении. Защита целостности информации при обработке. Защита целостности информации при транспортировке. Защита от угрозы нарушения целостности информации на уровне содержания. Построение систем защиты от угрозы отказа доступа к информации. Защита семантического анализа и актуальности информации.

В РАМКАХ ДАННОЙ ТЕМЫ ПРЕДУСМОТРЕНЫ ПРАКТИЧЕСКИЕ ЗАНЯТИЯ.

### Вопросы практического занятия:

ПЗ: Исследование шифра скользящей перестановки с использованием реализации XY-Mover. Изучение устойчивых закономерностей открытого текста и их использование при дешифровании простой замены и перестановки. Этапы формирование алгоритма дешифрования. Шифрующий автомат скользящей перестановки.

ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПРЕДЛАГАЮТСЯ СЛЕДУЮЩИЕ ВОПРОСЫ:

1). Какие существуют способы контроля целостности сообщений при взаимном доверии сторон?
2). Как контролировать целостность сообщений при высоком уровне помех в каналах связи?
3). Как организован обмен документами, заверенными цифровой подписью?
4). В чем отличие и сходство обычной и цифровой подписей?
5). Какими принципами нужно руководствоваться для сохранения целостности данных при их обработке?
6). Почему проблемы контроля целостности данных относятся к проблемам информационной безопасности?
7). Что означает контроль целостности данных на уровне содержания? Приведите примеры.
8). Как обеспечить целостность данных при их хранении?
9). Что такое надежность и чем отличается надежность аппаратуры от надежности программного обеспечения?
10). Как защитить программное обеспечение от изучения логики его работы?
11). Предложите меры по обеспечению более надежной работы ЛВС университета.

12). Каковы способы повышения надежности аппаратуры и линий связи?

ТЕМА 6. ПОЛИТИКА И МОДЕЛИ БЕЗОПАСНОСТИ.

Политика безопасности. Субъектно-объектные модели разграничения доступа. Аксиомы политики безопасности. Политика и модели дискреционного доступа. Парольные системы разграничения доступа. Политика и модели мандатного доступа. Теоретико-информационные модели. Политика и модели тематического разграничения доступа. Ролевая модель безопасности.

В РАМКАХ ДАННОЙ ТЕМЫ ПРЕДУСМОТРЕНЫ ПРАКТИЧЕСКИЕ ЗАНЯТИЯ.

Вопросы практического занятия:
ПЗ: Получить представление об общих принципах построения и использования программных средств защиты информации, в частности с программой PGP (Pretty Good Privacy). Освоение средств программной системы PGP, предназначенных для шифрования конфиденциальных ресурсов и разграничения доступа к ним, а также для обеспечения целостности информационных ресурсов с помощью механизма электронной цифровой подписи.

ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПРЕДЛАГАЮТСЯ СЛЕДУЮЩИЕ ВОПРОСЫ:

1). Что такое политика безопасности, кто ее разрабатывает и где она применяется?
2). Приведите классификацию моделей разграничения доступа. Какова их роль в теории информационной безопасности?
3). Каковы основные достоинства и недостатки дискреционных моделей?
4). Приведите примеры использования дискреционных моделей разграничения доступа.
5). Что такое монитор безопасности и какие требования к нему предъявляются?
6). Перечислите основные положения субъектно-объектного подхода к разграничению доступа? В чем достоинства и недостатки такого подхода?
7). В чем суть мандатной политики разграничения доступа?
8). Каковы основные достоинства и недостатки мандатной политики?
9). Что такое скрытые каналы утечки информации и как их обнаружить?
10). В чем суть моделей группового доступа?

ТЕМА 7. ОБЗОР МЕЖДУНАРОДНЫХ СТАНДАРТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. Европейские критерии безопасности информационных технологий (ITSEC). Федеральные критерии безопасности информационных технологий США. Единые критерии безопасности информационных технологий. Группа международных стандартов 270000.

В РАМКАХ ДАННОЙ ТЕМЫ ПРЕДУСМОТРЕНЫ ПРАКТИЧЕСКИЕ ЗАНЯТИЯ.

Вопросы практического занятия:
ПЗ: Изучение способов контроля правильности передачи данных. Код с проверкой на четность. Коды Хэмминга. Циклические коды. Общие положение эффективного кодирования информации.

ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПРЕДЛАГАЮТСЯ СЛЕДУЮЩИЕ ВОПРОСЫ:

1). Цели применения стандартов информационной безопасности.
2). Охарактеризуйте основные положения Оранжевой книги.
3). Почему в современных стандартах отказываются от единых шкал, характеризующих уровень безопасности?
4). Каковы основные положения Европейских критериев безопасности информационных технологий?
5). Чем отличаются «информационная система» и «продукт информационных технологий»?
6). Для чего вводятся критерии адекватности?
7). Что такое Профиль защиты?
8). В чем особенности Канадских критериев безопасности компьютерных систем?

9). Опишите структуру Общих критериев безопасности информационных технологий.
10). Опишите технологию применения Общих критериев безопасности информационных технологий.
11). Каковы тенденции развития международной нормативной базы в области информационной безопасности?

ТЕМА 8. ИНФОРМАЦИОННЫЕ ВОЙНЫ И ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО.

Определение и основные виды информационных войн. Информационно-техническая война. Информационно-психологическая война.

В РАМКАХ ДАННОЙ ТЕМЫ ПРЕДУСМОТРЕНЫ ПРАКТИЧЕСКИЕ И ЛАБОРАТОРНЫЕ ЗАНЯТИЯ.

Вопросы практического занятия:
ПЗ: Методы сжатия по Шеннону и Хаффмену. Основные методы обратимого и необратимого сжатия. Алгоритмы компрессии и декомпрессии.

ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПРЕДЛАГАЮТСЯ СЛЕДУЮЩИЕ ВОПРОСЫ:

1). Чем отличаются понятия «информационная война» и «информационное противоборство»?
2). Чем отличается информационная война от обычного вооруженного конфликта?
3). Какие виды информационных войн Вы можете выделить?
4). Приведите пример межкорпоративной информационной войны.
5). Можно ли рассматривать рекламу как средство ведения информационной борьбы?
6). Какие приемы ведения информационной войны используются во время предвыборных кампаний, приведите примеры.
7). Что такое информационное оружие? Какие виды оружия применяются в ходе ведения информационной войны? Каковы цели информационной войны?
8). Каковы средства и методы защиты от информационно-технического оружия?
9). Каковы особенности информационно-психологической войны?

## 4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 4.1. ОСНОВНАЯ ЛИТЕРАТУРА


1. Медведев, В. А., Информационная безопасность. Введение в специальность + еПриложение:Тесты : учебник / В. А. Медведев. — Москва : КноРус, 2024. — 143 с. — ISBN 978-5-406-12625-7. — URL: https://book.ru/book/951878 — Текст : электронный.
2. Николаев, Н. С., Управление информационной безопасностью: учебник / Н. С. Николаев. — Москва: КноРус, 2021. — 188 с. — ISBN 978-5-406-07325-4. — URL: https://book.ru/book/939841 — Текст: электронный.
3. Мельников, В. П., Информационная безопасность : учебник / В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. — Москва : КноРус, 2023. — 371 с. — ISBN 978-5-406-11960-0. — URL: https://book.ru/book/950148 — Текст: электронный.


### 4.2. ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА


4. Верещагина, Е. А., Исследование проблем информационной безопасности в банковской сфере : монография / Е. А. Верещагина, А. Л. Золкин, А. В. Фролов. — Москва: Русайнс, 2023. — 177 с. — ISBN 978-5-466-03976-4. — URL: https://book.ru/book/950915 — Текст : электронный.
5. Бабаш, А. В., Информационная безопасность. Лабораторный практикум + еПриложение : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. — Москва : КноРус, 2023. — 131 с. — ISBN 978-5-406-11731-6. — URL: https://book.ru/book/949452 — Текст : электронный.
6. Крылов, Г. О., Базовые понятия информационной безопасности: учебное пособие / Г. О. Крылов, С. Л. Ларионова, В. Л. Никитина. — Москва: Русайнс, 2023. — 257 с. — ISBN 978-

5-466-01996-4. — URL: https://book.ru/book/946979 — Текст : электронный.
7. Ищейнов, В. Я., Информационная безопасность и защита информации: словарь терминов и понятий : словарь / В. Я. Ищейнов. — Москва : Русайнс, 2024. — 226 с. — ISBN 978-5-466-04502-4. — URL: https://book.ru/book/951881 — Текст: электронный.

### 4.3. СОСТАВ ЛИЦЕНЗИОННОГО И СВОБОДНО РАСПРОСТРАНЯЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, В ТОМ ЧИСЛЕ ОТЕЧЕСТВЕННОГО ПРОИЗВОДСТВА

| № | Наименование лицензионного продукта |
|---|---|
| 1. | Microsoft Windows 7 Pro |
| 2. | Office 2007 Standard |
| 3. | Moodle 3.8 |
| 4. | Oracle VM VirtualBox 6 |
| 5. | AutoCAD 2012 AcademicEdition New SLM ML03 |

### 4.4. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ, ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ, ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ

1. Информационно-правовой портал «Гарант» http://www.garant.ru/
2. Справочная правовая система КонсультантПлюс http://www.consultant.ru/
3. Федеральный портал «Российское образование» https://www.edu.ru/
4. Система автоматизации библиотек ИРБИС64; ООО «ЭйВиДи–систем» http://support.open4u.ru
5. Электронная библиотечная система ООО «КноРус медиа» www.book.ru
6. Электронная библиотечная система издательства «Лань» www.e.lanbook.ru

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКИЕ УСЛОВИЯ, ОБОРУДОВАНИЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ

Для проведения обучения необходимы:

- лекционная аудитория, оборудованная комплектом мебели, доской, и проекционным мультимедийным оборудованием;
- учебная аудитория с компьютерами, оснащенными операционной системой Windows и пакетом программ Microsoft Office и имеющими доступ к сети Интернет и ЭИОС ГГАУ;
- библиотека с информационными ресурсами на бумажных и электронных носителях.

## 6. ОЦЕНОЧНЫЕ СРЕДСТВА

6.1 Перечень вопросов (к зачету).

### ВОПРОСЫ К ЗАЧЕТУ

1. Защита информации в России (периоды, факторы влияния, деятельность по защите, органы защиты).
2. Перспективные направления исследований в области информационной безопасности.
3. В каких направлениях идет развитие теории информационной безопасности в настоящее время?
4. Каков вклад российских ученых в теорию информационной безопасности?
5. Информационные ресурсы. Классификация информационных ресурсов.

6. Перечислите основные носители информации, особенности их использования и защиты.
7. Какие критерии оценки ценности информации Вы можете предложить?
8. Приведите примеры различной зависимости ценности информации от времени.
9. Что понимается под информационными ресурсами?
10. Что понимается под конфиденциальной информацией?
11. Какие существуют виды тайны?
12. Какое назначение имеет перечень конфиденциальных сведений предприятия?
13. Каково место информационной безопасности в системе национальной безопасности Российской Федерации?
14. Сформулируйте основные положения Доктрины информационной безопасности РФ.
15. Каковы основные задачи в области информационной безопасности?
16. Кто несет ответственность за нарушение режима защиты информации?
17. Каковы функции руководителей предприятий при организации защиты информации?
18. Покажите роль различных министерств и ведомств в вопросах защиты информации.
19. Приведите примеры систем, для которых наибольшую угрозу безопасности представляет нарушение конфиденциальности информации.
20. В каких системах на первом месте стоит обеспечение доступности информации?
21. В чем различие понятий «нарушение конфиденциальности информации», «несанкционированный доступ к информации», «утечка информации»?
22. В чем отличие терминов «Несанкционированного доступа» и «Нарушение конфиденциальности информации»?
23. Что понимается под утечкой информации? Каким образом классифицируются каналы утечки информации?
24. Каким образом следует выбирать меры защиты конфиденциальности информации?
25. Дайте определение идентификации и аутентификации пользователя. В чем разница между этими понятиями?
26. Какие основные методы контроля доступа используются в известных вам информационных системах? В чем их достоинства и недостатки?
27. Почему аутентификация с использованием пароля считается в настоящее время ненадежной?
28. Каковы методы аутентификации с использованием предметов заданного типа? Назовите те, которые получили распространение в последнее время.
29. Дайте определение шифра и сформулируйте основные требования к нему. Поясните, что понимается под совершенным шифром.
30. Как организован обмен документами, заверенными цифровой подписью?
31. В чем отличие и сходство обычной и цифровой подписей?
32. Какими принципами нужно руководствоваться для сохранения целостности данных при их обработке?
33. Что означает контроль целостности данных на уровне содержания? Приведите примеры.
34. Как обеспечить целостность данных при их хранении?
35. Предложите меры по обеспечению более надежной работы ЛВС университета.
36. Что такое политика безопасности, кто ее разрабатывает и где она применяется?
37. Приведите примеры использования дискреционных моделей разграничения доступа.
38. Что такое монитор безопасности и какие требования к нему предъявляются?
39. Перечислите основные положения субъектно-объектного подхода к разграничению доступа? В чем достоинства и недостатки такого подхода?
40. Что такое скрытые каналы утечки информации и как их обнаружить?
41. Цели применения стандартов информационной безопасности.
42. Охарактеризуйте основные положения Оранжевой книги.

43. Каковы основные положения Европейских критериев безопасности информационных технологий?
44. Чем отличаются «информационная система» и «продукт информационных технологий»?
45. Для чего вводятся критерии адекватности?
46. В чем особенности Канадских критериев безопасности компьютерных систем?
47. Опишите структуру Общих критериев безопасности информационных технологий.
48. Каковы тенденции развития международной нормативной базы в области информационной безопасности?
49. Чем отличаются понятия «информационная война» и «информационное противоборство»?
50. Какие виды информационных войн Вы можете выделить?
51. Приведите пример межкорпоративной информационной войны.
52. Какие приемы ведения информационной войны используются во время предвыборных кампаний, приведите примеры.
53. Что такое информационное оружие? Какие виды оружия применяются в ходе ведения информационной войны?
54. Каковы цели информационной войны? Каковы средства и методы защиты от информационно-технического оружия?
55. Каковы особенности информационно-психологической войны?

6.2 Тестовые задания для диагностической работы.

ТЕСТ по теме:
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЗАЩИТА ИНФОРМАЦИИ

1. Исключительное право на произведение действует:
   A). в течение всей жизни автора и 50 лет после его смерти
   B). в течение всей жизни автора и 70 лет после его смерти
   C). в течение всей жизни автора и 100 лет после его смерти
   D). в течение всей жизни автора и 40 лет после его смерти

2. Совокупность наиболее значимых решений, направленных на обеспечение приемлемого уровня безопасности функционирования предприятия, — это:
   A). система безопасности
   B). стратегия безопасности
   C). политика безопасности

3. Большинство атак на узлы сети реализуется:
   A). путем атак на серверы и устройства, установленные внутри DMZ
   B). путем атак межсетевого экрана и вмешательства в трафик, проходящий через него
   C). по коммутируемым каналам
   D). изнутри корпоративной сети
4. Право_____ состоит в том, что автор произведения изобразительного искусства имеет право на получение вознаграждения в виде процентных отчислений от цены перепродажи оригинала произведения.

5. Технический канал утечки информации путем «высокочастотного навязывания» наиболее часто используют для перехвата разговоров, ведущихся в помещении:

A). через телефонный аппарат
B). через системы отопления и водоснабжения
C). через сети электропитания

6. Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, должны быть направлены на обеспечение конфиденциальности, _____ и доступности информации.

7. Целью атаки типа IP-спуфинг является:
   A). отказ в обслуживании
   B). получение всех пакетов, принимаемых сетевой картой жертвы
   C). попытка выдать себя за санкционированного пользователя
   D). внесение сторонних команд или данных в работающую систему с целью изменения хода ее работы

8. RBAC/Web может использоваться с веб-серверами:
   A). только под Windows
   B). на практически всех операционных системах
   C). только под UNIX

9. Системы анализа защищенности на уровне СУБД чаще всего исполняются _____.

10. Для безопасной передачи сеансовых ключей («handshaking») при организации пиринговой сети с криптозащитой применяется:
    A). алгоритм AES
    B). шифр SEAL
    C). алгоритм 3DES
    D). асимметричный алгоритм шифрования

11. Основным направлением противодействия утечке информации является обеспечение физической и _____ защиты информационных ресурсов.

12. Инвентаризацией служб и установленного ПО занимаются:
    A). средства непрерывного мониторинга сети и отдельных ее узлов
    B). средства, позволяющие оценить защищенность сети в целом
    C). средства, реализующие основные защитные механизмы

13. Для обнаружения и локализации радиоизлучающих специальных технических средств может использоваться:
    A). Локатор нелинейностей NJE-4000 (Орион)
    B). Система «Шторм-7»
    C). Детектор поля ST007
    D). Система защиты «Гром ЗИ-4А»

14. Работа всех брандмауэров основана на использовании информации разных уровней:

A). OSI
B). TCP/IP
C). DOD
D). IPX/SPX

15. Авторами аудиовизуального произведения являются:
    A). композитор
    B). автор сценария
    C). актеры
    D). режиссер-постановщик
    E). исполнители музыки

16. Электромагнитные излучения элементов ТСОИ, носителем информации является электрический ток, сила которого, напряжение, частота или фаза изменяются по закону информационного сигнала, могут использоваться для съема информации:
    A). с дисплея по электромагнитному каналу
    B). с сетевых подключений
    C). с принтера по каналу связи с компьютером
    D). за счет побочного излучения терминала