Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Троицкий Александр Витальевич

Подписано цифровой подписью: Троицкий Александр Витальевич

**«УТВЕРЖДАЮ»**
**И.о. проректора**
**_____ А.В. Троицкий**
**«___»_____2023 г.**

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ**

**КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

# РАБОЧАЯ ПРОГРАММА
# ДИСЦИПЛИНЫ (МОДУЛЯ)

## Б1.В.08 «ИНФОРМАЦИОННО – АНАЛИТИЧЕСКИЕ СИСТЕМЫ БЕЗОПАСНОСТИ»

**Направление подготовки: 10.04.01 - Информационная безопасность**

**Направленность (профиль): Менеджмент информационной безопасности**

**Уровень высшего образования: Магистратура**

**Форма обучения: очная**

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

**Автор: Сухотерин А.И. Рабочая программа дисциплины (модуля): Информационно-аналитические системы безопасности. – Королев МО: «Технологический Университет», 2023**

Рецензент:Соляной В.Н.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего профессионального образования (ФГОС ВО) по направлению подготовки магистров 10.04.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

**Рабочая программа рассмотрена и одобрена на заседании кафедры:**

| | | | | |
|---|---|---|---|---|
| Заведующий кафедрой (ФИО, ученая степень, звание, подпись) | Соляной В.Н. к.в.н. доцент | | | |
| Год утверждения (переутверждения) | 2023 | 2024 | | |
| Номер и дата протокола заседания кафедры | № 8 от 29.03.2023г. | | | |

**Рабочая программа согласована:**
**Руководитель ОПОП ВО** Сухотерин А.И.

**Рабочая программа рекомендована на заседании УМС:**

| | | | | |
|---|---|---|---|---|
| Год утверждения (переутверждения) | 2023 | 2024 | | |
| Номер и дата протокола заседания УМС | Протокол № 5 от 11.04.2023г. | | | |

## 1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП

**Целью** изучения дисциплины является:

1. Научить студентов решать задачи связанные с созданием, эксплуатацией, развитием и защитой автоматизированных ИАС, обеспечивающих отработку и анализ специальной информации в процессе информационно – аналитической деятельности в интересах региона
2. Дать представление об учете и использовании особенностей информационных технологий, применяемых в автоматизированных ИАС, для информационно-аналитического обеспечения мониторинга
3. Уметь, формировать и реализовывать комплекс мероприятий по защите информации в автоматизированных ИС информационной безопасности.

В процессе обучения по направлению подготовки 10.04.01 «Информационная безопасность», студент приобретает и совершенствует следующие компетенции:

**Профессиональные компетенции:**

- ПК-1: Способен организовывать выполнение работ, управлять коллективом автоматизированных ИАС в защищенном исполнении.
- ПК-3: Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности.

Основными **задачами** дисциплины являются:

1. Научить студентов проводить анализ и исследовать модели автоматизированных ИС, обеспечивающих обработку и анализ специальной информации в целях принятия решений в процессе ИА деятельности (специальные ИАС);
2. Научить применять на практике стандарты, относящиеся к обеспечению информационной безопасности;
3. Проводить синтез и анализ проектных решений по ИА обеспечению информационной безопасности;
4. Обеспечить эффективное применение информационно-технологических ресурсов с учетом нормативных требований по защите информации;
5. Разрабатывать и реализовывать политики информационной безопасности для ИАС различно назначения;
6. Участвовать в проектировании и эксплуатации системы управления информационной безопасностью;
7. Разрабатывать предложения по совершенствованию системы управления информационной безопасностью;

8. Формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной АИС;

9. Применять модели, методы и методики информационно – аналитической деятельности, реализуемые с применением ИАС.

Показатель освоения компетенции отражают следующие индикаторы:

**Трудовые действия:**

- ПК-1.3. Управлять работой коллектива профессионалов ИБ, разрабатывать нормативно-методические документы по функционированию автоматизированной ИАС, формировать комплекс мер по информационной защите автоматизированной ИАС с разработкой частных политик безопасности компьютерных систем.
- ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда.

**Необходимые умения:**

- ПК-1.1. Знать научные основы, методы и технологии управленческой деятельности, нормативную базу по созданию и эксплуатацию защищенных автоматизированных ИАС, принципы и методы организации работ по ЗИ в ИАС, основные средства и способы организационного обеспечения ИБ, источники и классификацию угроз ИБ.
- ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении.

**Необходимые знания:**

- ПК-1.2. Работать в коллективе, разрабатывать организационно-управленческие документы, принимать управленческие решения, реализовывать целесообразные меры противодействия информационным угрозам с применением национальных и международных стандартов в области ЗИ, оценивать их эффективность.
- ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок.

## 2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП ВО

Дисциплина относится к дисциплинам части, формируемой участниками образовательных отношений, блока 1 основной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на одновременно изучаемых дисциплинах: «Методы и средства обеспечения безопасного доступа к информационным ресурсам», «Защищенные информационные системы» и компетенциях: ПК-2, 3; УК-1; ОПК-1.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при совместном изучении дисциплин общенаучного цикла «Комплексная проверка информационной безопасности», и выполнения выпускной квалификационной работы

## 3.Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 2 зачетные единицы, 72 часа.

**Таблица1**

| Виды занятий | Всего часов | Семестр 3 | Семестр … | Семестр … | Семестр … |
|---|---|---|---|---|---|
| **Общая трудоемкость** | 72 | 72 | | | |
| **ОЧНАЯ ФОРМА ОБУЧЕНИЯ** | | | | | |
| **Аудиторные занятия** | 46 | 46 | | | |
| Лекции (Л) | 16 | 16 | | | |
| Практические занятия (ПЗ) | 16 | 16 | | | |
| Лабораторные работы (ЛР) | 8 | 8 | | | |
| Другие виды контактной работы* | 6 | 6 | | | |
| Практическая подготовка | 4 | 4 | | | |
| **Самостоятельная работа** | 26 | 26 | | | |
| **Курсовые работы (проекты)** | - | - | | | |
| **Расчетно-графические работы** | - | - | | | |
| **Контрольная работа, домашнее задание** | + | + | | | |
| **Текущий контроль знаний (7 - 8, 15 - 16 недели)**- 2ч. | - | -- | | | |
| **Вид итогового контроля** | Зачет | Зачет | | | |

* Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование.

# 1. Содержание дисциплины

## 4.1.Темы дисциплины и виды занятий

**Таблица 2**

| Наименование тем | Лекции, час. | Практич. занятия, час. | Лабораторные работы, час. | Занятия в интерактивной форме, час. | Пр. подг. час. | Код компетенций |
|---|---|---|---|---|---|---|
| | **третий семестр** | | | | | |
| | Раздел 1. Основы проектирования и внедрения ИАС безопасности региона | | | | | |
| Тема 1. Информационно – аналитическое обеспечение деятельности информационной безопасности региона | 1 | 1 | 1 | 2 | - | ПК-1 |
| Тема 2. Особенности организации регионального управления информационной безопасностью (требования к работе информационно – аналитических подразделений) | 1 | 2 | 0.5 | 2 | - | ПК-1 |
| Тема 3. Основы построения систем информационно – аналитического обеспечения управления безопасностью в органах государственной власти и местного самоуправления региона | 1 | 1.5 | 0.5 | 1 | - | ПК-1 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Тема 4. Инструментарий информационно – аналитической поддержки принятия решений в органах государственной власти и местного самоуправления региона | 1 | 1.5 | 0.5 | 1 | - | ПК-1 |
| Тема 5. Методология анализа информации при подготовке информационно – аналитических материалов в органах государственной власти и местного самоуправления региона | 2 | 2 | 0.5 | 1 | - | ПК-1 |
| Тема 6. Организационно – распорядительные документы по вводу региональной информационно - аналитической системы ИБ в эксплуатацию | 2 | 1.5 | 1 | 1 | 2 | ПК-1 |
| | Раздел 2. Информация: сбор, защита, анализ для региональной ИАС безопасности | | | | | |
| Тема 7. Мониторинг. Прогнозирование. Задачи прогнозирования в органах государственной власти и местного самоуправления региона | 2 | 2 | 1 | 1 | - | ПК-1 ПК-3 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Тема 8. Технические средства аналитической разведки. | 2 | 1.5 | 1 | 1 | - | ПК-1 ПК-3 |
| Тема 9. Методика информационно-аналитической работы. | 2 | 1.5 | 1 | 1 | - | ПК-1 ПК-3 |
| Тема 10. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность в органах государственной власти и местного самоуправления региона. | 2 | 1.5 | 1 | 1 | 2 | ПК-1 ПК-3 |
| Итого: | 16 | 16 | 8 | 12 | 4 | |

## 4.2. Содержание тем дисциплины

### Раздел 1. Основы проектирования и внедрения ИАС безопасности региона

**Тема 1. Информационно – аналитическое обеспечение деятельности информационной безопасности региона**

Информационно – аналитическое обеспечение деятельности органов власти. Общие подходы. Специфика принятия решений в органах управления и основные проблемы создания комплексных систем информационно – аналитического обеспечения деятельности органов власти.

**Тема 2. Особенности организации регионального управления информационной безопасностью (требования к работе информационно – аналитических подразделений)**

Стратегический уровень регионального управления. Оперативное управление. Управление в условиях черезвычайных ситуаций. Требования к работе информационно – аналитических подразделений органов управления.

**Тема 3. Основы построения систем информационно – аналитического обеспечения управления безопасностью в органах государственной власти и местного самоуправления региона**

Информационно-аналитическая система поддержки принятия решений руководителем субъекта российской Федерации. Основы построения систем информационно – аналитического обеспечения управления регионом на

примере Санкт-Петербурга. Функциональная структура системы информационно – аналитического обеспечения и ее место в управлении регионом.

**Тема 4. Инструментарий информационно – аналитической поддержки принятия решений в органах государственной власти и местного самоуправления региона**

Нормативно – правовое обеспечение работ по подготовке информационно – аналитических материалов. Виды информационно – аналитических материалов и Виды информационно – аналитических материалов.

**Тема 5. Методология анализа информации при подготовке информационно – аналитических материалов в органах государственной власти и местного самоуправления региона**

Методология анализа информации при подготовке информационно-аналитических материалов. Применение методов анализа информации и моделирование процессов жизнедеятельности (на основе опыта эксплуатации ИАО)

**Тема 6. Организационно – распорядительные документы по вводу региональной информационно - аналитической системы ИБ в эксплуатацию**

Интерпритация результатов исследуемой проблемы возможным вариантам управленческих решений. Подготовка информационно – аналитических материалов и создание дизайна

## Раздел 2. Информация: сбор, защита, анализ для региональной ИАС безопасности

**Тема 7. Мониторинг. Прогнозирование. Задачи прогнозирования в органах государственной власти и местного самоуправления региона**

Общие представления о мониторинге. Стратегический мониторинг. Оперативный мониторинг. Задачи разведывательного мониторинга. Мониторинг средств массовой информации. Мониторинг массовых настроений. Мониторинг массовой активности. Мониторинг учреждений. Мониторинг ведущих деятелей. Системы обнаружения. Системы оперативного информирования. Феномен предсказывания. Возможности предсказывания. Ясновидение. Система прогнозирования. Структура прогноза. Метод имитационного моделирования. Метод Делфи. Метод морфологического анализа. Метод "дерева целей". Неформальное прогнозирование. Думание за противника. Место прогнозирования в системе деятельности. Прогнозирование индивидуума. Прогнозирование массовых настроений. Прогнозирование выборов. Прогнозирование событий. Тактическое прогнозирование. Стратегическое прогнозирование.

**Тема 8. Технические средства аналитической разведки**

Поддержка решений. Системы оперативного прогнозирования. Экспертные системы. Системы поддержки нетипового анализа числовых данных. Системы для контент - анализа. Системы для фильтрования

данных. Системы поддержки неформального анализа текстов. Базы данных аналитической разведки. Интернет как средство разведки и влияния. Мониторинг в интернете. Направленный поиск в интернете. Управление поиском в интернете. Управление доступом в интернет. Управление хостингом. Управление дискуссиями на интернет - форумах. Управление электронной почтой. Рассылка электронных сообщений. Индивидуальное использование интернета. Поиск в интернете. "Активная" деятельность в интернете. Способы повышения эффективности Личная информационная система. Использование компьютера. Теория влияния. Манипулирование руководителями. Нейтрализация руководителей. Манипулирование массами. Поддержка интеллектуалов. Нейтрализация активистов. Влияние на выборы. Противодействие влиянию на аналитическую разведку. Противодействие влиянию на руководителей. Противодействие влиянию на общество в целом.

**Тема 9. Методика информационно-аналитической работы**

Логика процесса исследования. Информационная работа. Основные этапы информационно-аналитической работы. Работа с источниками информации. Планирование работы. Начало работы. Способы работы. Поиск информации. Документальные источники информации. Работа с книгой. Техника чтения.

**Тема 10. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность в органах государственной власти и местного самоуправления региона**

Источники информации. Обретение доступа к документам. Перехват и перлюстрация писем. Обработка «мусора». Техника интерпретации данных. Обеспечение безопасности и защиты информации. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность

## 5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

## 6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Информационно-аналитические системы безопасности» приведена в Приложении 1.

## 7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

**Основная литература:**

1. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: https://doi.org/10.29039/01848-4. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232287 (дата обращения: 03.10.2022). – Режим доступа: по подписке.
2. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

**Дополнительная литература:**

1. Коноплева, И. А. Управление безопасностью и безопасность бизнеса : учебное пособие для вузов / И. А. Коноплева, И. А. Богданов ; под ред. И. А. Коноплевой. — Москва : ИНФРА-М, 2020. — 448 с. — (Высшее образование). - ISBN 978-5-16-003230-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1068834 (дата обращения: 03.10.2022). – Режим доступа: по подписке.
2. Федотова, Е. Л. Информационные технологии и системы : учебное пособие / Е. Л. Федотова. — Москва : ФОРУМ : ИНФРА-М, 2022. — 352 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0927-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1839925 (дата обращения: 03.10.2022). – Режим доступа: по подписке.
3. Меняев, М. Ф. Цифровая экономика предприятия : учебник / М.Ф. Меняев. — Москва : ИНФРА-М, 2021. — 369 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1045031. - ISBN 978-5-16-015656-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1217285 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

## 8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

**Интернет-ресурсы**:

1. www.biblioclub.ru - Универсальная библиотека онлайн.
2. www.rucont.ru - ЭБС «Руконт».
3. http://www.academy.it.ru/ – академия АЙТИ.
4. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
5. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации
6. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности
7. http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

## 9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

## 10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

- **Перечень программного обеспечения:** MSOffice.

- **Информационные справочные системы:**
  1.Электронные ресурсы образовательной среды университета
  2.Информационно-справочные системы:
  Консультант+;
  Гарант.

## 11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

**Лекционные занятия**:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы.

**Практические занятия:**

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;

- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Задания

**ЗАДАЧА 1.**

Холдинговая компания «ПОЛИМЕТ» имеет головное предприятие и несколько дочерних фирм в ряде городов России и за рубежом. В структуру холдинга входит коммерческий банк. Основной деятельностью «ПОЛИМЕТА» является переработка металлургического сырья, производство изделий из металла, торговля сырьем и изделиями из металла. Головным предприятием владеют несколько человек. Они же владеют контрольными пакетами акций всех дочерних предприятий. Обороты холдинга исчисляются миллиардами рублей. На рынке металла, как в стране, так и за рубежом идет жесткая конкуренция. Условия торговли металлами предельно строгие и требуют постоянного взаимодействия с контролирующими и проверяющими органами. Необходимо постоянное оформление квот, лицензий и других разрешительных документов. Торговля металлами требует больших объемов железнодорожных и морских перевозок.

**ВОПРОСЫ:**

- 1. Какие задачи могут стоять перед Службой Конкурентной Разведки (СКР) исходя из условий работы холдинга, его структуры, оборотов, особенностей рынка?
- 2. Какая оптимальная структура Службы Конкурентной Разведки может быть выбрана в соответствии с определенными для СКР задачами?

**ЗАДАЧА 2.**

Фирма «ЛИНДА» занимается оказанием информационных и консалтинговых услуг в области новых технологий. Основное внимание уделяет конверсионным разработкам, нс имеющим аналогов в мире. Она собирает информацию о наиболее перспективных научных разработках, позволяющих наладить производство высоко ликвидной на западном рынке продукции.

Фирма занимается привлечением инвестиций, решает вопросы оформления патентов на изобретения и организации производства.

В фирме работает небольшой штат (20 человек) постоянных сотрудников и привлекается более 100 специалистов по трудовым соглашениям.

**ВОПРОСЫ:**

- 1. Какие задачи могут стоять перед Службой Конкурентной Разведки исходя из условий работы фирмы, ее структуры, особенностей рынка?
- 2. Какая оптимальная структура СКР может быть выбрана в соответствии с определенными для СКР задачами?

**ЗАДАЧА 3.**

Производственно-коммерческая фирма «АВЕКС» решила создать СКР для защиты своих интересов. Вас пригласили создать СКР и организовать ее работу для решения следующих задач:

физической охраны помещений и защиты руководителей от конкурентной разведки;

инженерной защиты офиса и производственных помещений от несанкционированного доступа конкурентов к информационным ресурсам фирмы;

информационного освещения деятельности партнеров и конкурентов, в том числе зарубежных.

**ВОПРОС:**

Какие предприятия и организации вы хотели бы привлечь к работе, и какие вопросы вы предполагаете решать с ними?

**ЗАДАЧА 4.**

Холдинговая компания «Глобус» специализируется на международных транспортных перевозках. В одном из западноевропейских дочерних предприятий, работающих в тесном партнерстве с предприятием, расположенном в российском порту, произошло чрезвычайное происшествие - покушение на директора. Директор тяжело ранен. Состояние дел в предприятии неважное: прибыли нет, большая текучесть кадров.

Руководство холдинга поручило СКР разобраться с положением, защитить интересы фирмы, обеспечить безопасность персонала.

**ВОПРОС:**

При отработке версий и выполнении задания к кому необходимо было бы обратиться за помощью и какие вопросы решать?

**ЗАДАЧА 5.**

Торговая компания г. Томска закупила в Москве партию изделий бытовой электроники общим объемом около 5 грузовых автомобилей. По условиям контракта товар продавался со склада в Москве, далее самовывозом. Полную партию товара продавец обязался поставить в течение недели частями.

Покупатель решил везти груз на автомобилях, арендованных в Московских транспортных агентствах.

Охрану груза было поручено осуществлять СБ компании.

**ВОПРОС:**

Какие меры следует предпринять СБ компании для обеспечения сохранности груза?

**ЗАДАЧА 6.**

Коммерческий банк «Развитие» по личной рекомендации Председателя союза банков принял в качестве клиента ТОО «Веста», где учредителями были российская гражданка и турецкий гражданин. Через некоторое время турок объявил, что готовит очень крупный контракт по строительству индивидуальных коттеджей и попросил кредит на 40 млн. рублей. Так как в залог он представить ничего не мог, за него выступил с ходатайством «по дружбе» Председатель союза. Еще через некоторое время он попросил кредит на 80 млн. руб. и в качестве залога предложил арендный договор на землю. Получив кредиты, турок перестал вести расчеты через этот банк и вскоре объявил о закрытии фирмы.

Предварительным расследованием СКР банка установлено, что кредит турок использовал на другие нужды. Денег на счету новой фирмы почти нет. Арендный договор на землю был оформлен с грубейшими нарушениями закона в сговоре с председателем колхоза. В финансовых документах отмечается умышленное искажение отчетности, налоги нс платились. Существенную поддержку турку оказывал бывший руководящий сотрудник правоохранительного министерства.

**ВОПРОСЫ:**

- 1. Какие предупредительные меры нужно было предпринять СКР в отношении гражданина Турции?
- 2. По каким направлениям следует вести разработку турка, чтобы поставить его перед необходимостью вернуть взятый кредит?

**ЗАДАЧА 7.**

Агропромышленная фирма «Юниор» имеет головное предприятие в Москве и несколько дочерних фирм в различных регионах России. К руководству фирмы «Юниор» на одной специализированной выставке обратился господин N, представившийся сотрудником известной зарубежной компании «АВС», с предложением об участии в совместном проекте в регионе, в котором «Юниор» имеет дочернюю фирму.

**ВОПРОСЫ:**

- 1. Какие мероприятия по проверке потенциального зарубежного партнера компании «АВС» должна провести Служба Конкурентной Разведки фирмы «Юниор»?
- 2. На какие моменты необходимо обратить особое внимание?

**Приложение 1**

**Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине**

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ**

**КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ) ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ БЕЗОПАСНОСТИ

**Направление подготовки: 10.04.01 - Информационная безопасность**
**Профиль: Менеджмент информационной безопасности**
**Уровень высшего образования: магистратура**
**Форма обучения: очная**

Королев
2023

# 1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

| № п/п | Индекс компе-тенции | Содержание компетенции | Раздел дисциплины, обеспечивающий формирование компетенции | В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобрести: | | |
|---|---|---|---|---|---|---|
| | | | | Трудовые действия | Необходимые умения | Необходимые знания |
| 1. | ПК-1 | Способен организовывать выполнение работ, управлять коллективом автоматизированных ИАС в защищенном исполнении. | Тема:1- 10 | ПК-1.3. Управлять работой коллектива профессионало в ИБ, разрабатывать нормативно-методические документы по функционированию автоматизированной ИАС, формировать комплекс мер по информационной защите автоматизированной ИАС с разработкой частных политик безопасности компьютерных систем. | ПК-1.2. Работать в коллективе, разрабатывать организационно-управленческие документы, принимать управленческие решения, реализовывать целесообразные меры противодействия информационным угрозам с применением национальных и международных стандартов в области ЗИ, оценивать их эффективность | ПК-1.1. Знать научные основы, методы и технологии управленческой деятельности, нормативную базу по созданию и эксплуатацию защищенных автоматизированных ИАС, принципы и методы организации работ по ЗИ в ИАС, основные средства и способы организационного обеспечения ИБ, источники и классификацию угроз ИБ. |
| 2 | ПК-3 | Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности. | Темы: 7-10 | ПК-3.3 Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда. | ПК-3.2 Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении. | ПК-3.1 Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок. |

## 2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

| *Код компетенции* | *Инструменты, оценивающие сформированность компетенции* | *Этапы и показатель оценивания компетенции* | *Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания* |
|---|---|---|---|
| ПК-1;ПК-3 | ***Тест*** | ***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов***<br>***Б) частично сформирована:***<br>• ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;***<br>• ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;***<br>***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов*** | ***Например:***<br>***Проводится письменно. Время, отведенное на процедуру - 30 минут.***<br>***Неявка – 0 баллов.***<br>***Критерии оценки определяются процентным соотношением.***<br>***Неудовлетворительно – менее 50% правильных ответов.***<br>***Удовлетворительно - от 51% правильных ответов.***<br>***Хорошо - от 70%.***<br>***Отлично – от 90%.***<br>***Максимальная оценка – 5 баллов.*** |
| ПК-1; ПК-3 | Доклад в форме презентации | ***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов***<br>***Б) частично сформирована:***<br>• ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;***<br>• ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;***<br>***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов*** | Проводится устно с использованием мультимедийных систем, а также с использованием технических средств<br>Время, отведенное на процедуру – 10 - 15 мин.<br>Неявка – 0.<br>Критерии оценки:<br>1.Соответствие представленной презентации заявленной тематике (1 балл).<br>2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл).<br>3.Владение информацией и способность отвечать на вопросы аудитории (1 балл).<br>4.Качество самой представленной презентации (1 балл).<br>5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).<br>Максимальная сумма баллов - 5 баллов.<br>Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал. |
| ПК-1; ПК-3 | Контрольная работа | ***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных*** | 1. Проводится устно в форме защиты отчета<br>2.Время, отведенное на процедуру – 10 - 15 мин.<br>Неявка – 0. |

| | | | |
|---|---|---|---|
| | | ***ответов***<br>***Б) частично сформирована:***<br>• ***компетенция освоена на продвинутом уровне – 70% правильных ответов;***<br>• ***компетенция освоена на базовом уровне – от 51% правильных ответов;***<br>***В) не сформирована (компетенция не сформирована) – менее 50% правильных ответов*** | Критерии оценки:<br>1.Соответствие оформления требованиям (1 балл).<br>2. Соответствие разработанного устройства<br>техническому заданию ( 1 балл)<br>3. Моделирование работы разработанного устройства ( 1 балл)<br>4. Качество и количество используемых источников ( 1 балл)<br>5. Правильность и полнота ответов на контрольные вопросы ( 1 балл)<br>Максимальная сумма баллов - 5 баллов.<br>Результаты оценочной процедуры представляются обучающимся непосредственно после защиты – для текущего контроля. Оценка проставляется в электронный журнал. |
| ПК-1; ПК-3 | Задачи | А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов<br>Б) частично сформирована:<br>• компетенция освоена на продвинутом уровне – 4 балла;<br>• компетенция освоена на базовом уровне – 3 балла;<br>В) не сформирована (компетенция не сформирована) – 2 и менее баллов | Например:<br>Проводится в письменной форме.<br>1. Выбор оптимального метода решения задачи (1 балл).<br>2. Умение применить выбранный метод (1 балл).<br>3. Логический ход решения правильный, но имеются арифметические ошибки в расчетах (1 балл).<br>4. Решение задачи и получение правильного результата (2 балла).<br>5. Задача не решена вообще (0 баллов).<br>Максимальная оценка – 5 баллов. |

## 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

***Примерная тематика докладов в форме презентаций:***

1. Информационно – аналитическое обеспечение деятельности органов власти. Общие подходы.
2. Специфика принятия решений в органах управления и основные проблемы создания комплексных систем информационно – аналитического обеспечения деятельности органов власти.
3. Стратегический уровень регионального управления. Оперативное управление. Управление в условиях черезвычайных ситуаций.
4. Требования к работе информационно – аналитических подразделений органов управления.

5. Информационно-аналитическая система поддержки принятия решений руководителем субъекта российской Федерации.

6. Основы построения систем информационно – аналитического обеспечения управления регионом на примере Санкт-Петербурга.

7. Функциональная структура системы информационно – аналитического обеспечения и ее место в управлении регионом.

8. Нормативно – правовое обеспечение работ по подготовке информационно – аналитических материалов.

9. Виды информационно – аналитических материалов и требования к их составу и содержанию.

10. Методология анализа информации при подготовке информационно- аналитических материалов.

11. Применение методов анализа информации и моделирование процессов жизнедеятельности (на основе опыта эксплуатации ИАО)

12. Интерпретация результатов исследуемой проблемы возможным вариантам управленческих решений. Подготовка информационно – аналитических материалов и создание дизайна

13. Общие представления о мониторинге. Стратегический мониторинг. Оперативный мониторинг. Задачи разведывательного мониторинга. Мониторинг средств массовой информации.

14. Мониторинг массовых настроений. Мониторинг массовой активности.

15. Мониторинг учреждений. Мониторинг ведущих деятелей.

16. Системы обнаружения. Системы оперативного информирования. Феномен предсказывания. Возможности предсказывания. Ясновидение.

17. Система прогнозирования. Структура прогноза. Метод имитационного моделирования. Метод Делфи.

18. Метод морфологического анализа. Метод "дерева целей". Неформальное прогнозирование. Думание за противника. Место прогнозирования в системе деятельности.

19. Прогнозирование индивидуума. Прогнозирование массовых настроений. Прогнозирование выборов. Прогнозирование событий.

20. Тактическое прогнозирование. Стратегическое прогнозирование.

21. Поддержка решений. Системы оперативного прогнозирования. Экспертные системы.

22. Системы поддержки нетипового анализа числовых данных. Системы для контент - анализа. Системы для фильтрования данных.

23. Системы поддержки неформального анализа текстов. Базы данных аналитической разведки. Интернет как средство разведки и влияния.

24. Мониторинг в интернете. Направленный поиск в интернете. Управление поиском в интернете.

25. Индивидуальное использование интернета. Поиск в интернете. "Активная" деятельность в интернете. Способы повышения эффективности

Личная информационная система. Использование компьютера. Теория влияния.

26. Манипулирование руководителями. Нейтрализация руководителей. Манипулирование массами. Поддержка интеллектуалов. Нейтрализация активистов. Влияние на выборы.

27. Противодействие влиянию на аналитическую разведку. Противодействие влиянию на руководителей. Противодействие влиянию на общество в целом.

28. Логика процесса исследования. Информационная работа. Основные этапы информационно-аналитической работы. Работа с источниками информации.

29. Планирование работы. Начало работы. Способы работы. Поиск информации. Документальные источники информации. Работа с книгой. Техника чтения.

30. Источники информации. Обретение доступа к документам. Перехват и перлюстрация писем.

31. Обработка «мусора». Техника интерпретации данных. Обеспечение безопасности и защиты информации.

32. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность

***Примерная тематика (контрольных заданий) задач для выполнения:***

**ЗАДАЧА 1.**

Холдинговая компания «ПОЛИМЕТ» имеет головное предприятие и несколько дочерних фирм в ряде городов России и за рубежом. В структуру холдинга входит коммерческий банк. Основной деятельностью «ПОЛИМЕТА» является переработка металлургического сырья, производство изделий из металла, торговля сырьем и изделиями из металла. Головным предприятием владеют несколько человек. Они же владеют контрольными пакетами акций всех дочерних предприятий. Обороты холдинга исчисляются миллиардами рублей. На рынке металла, как в стране, так и за рубежом идет жесткая конкуренция. Условия торговли металлами предельно строгие и требуют постоянного взаимодействия с контролирующими и проверяющими органами. Необходимо постоянное оформление квот, лицензий и других разрешительных документов. Торговля металлами требует больших объемов железнодорожных и морских перевозок.

**ВОПРОСЫ:**

- 1. Какие задачи могут стоять перед Службой Конкурентной Разведки (СКР) исходя из условий работы холдинга, его структуры, оборотов, особенностей рынка?

- 2. Какая оптимальная структура Службы Конкурентной Разведки может быть выбрана в соответствии с определенными для СКР задачами?

**ЗАДАЧА 2.**

Фирма «ЛИНДА» занимается оказанием информационных и консалтинговых услуг в области новых технологий. Основное внимание уделяет конверсионным разработкам, нс имеющим аналогов в мире. Она собирает информацию о наиболее перспективных научных разработках, позволяющих наладить производство высоко ликвидной на западном рынке продукции.

Фирма занимается привлечением инвестиций, решает вопросы оформления патентов на изобретения и организации производства.

В фирме работает небольшой штат (20 человек) постоянных сотрудников и привлекается более 100 специалистов по трудовым соглашениям.

**ВОПРОСЫ:**

- 1. Какие задачи могут стоять перед Службой Конкурентной Разведки исходя из условий работы фирмы, ее структуры, особенностей рынка?
- 2. Какая оптимальная структура СКР может быть выбрана в соответствии с определенными для СКР задачами?

**ЗАДАЧА 3.**

Производственно-коммерческая фирма «АВЕКС» решила создать СКР для защиты своих интересов. Вас пригласили создать СКР и организовать ее работу для решения следующих задач:

физической охраны помещений и защиты руководителей от конкурентной разведки;

инженерной защиты офиса и производственных помещений от несанкционированного доступа конкурентов к информационным ресурсам фирмы;

информационного освещения деятельности партнеров и конкурентов, в том числе зарубежных.

**ВОПРОС:**

Какие предприятия и организации вы хотели бы привлечь к работе, и какие вопросы вы предполагаете решать с ними?

**ЗАДАЧА 4.**

Холдинговая компания «Глобус» специализируется на международных транспортных перевозках. В одном из западноевропейских дочерних предприятий, работающих в тесном партнерстве с предприятием, расположенном в российском порту, произошло чрезвычайное происшествие - покушение на директора. Директор тяжело ранен. Состояние дел в предприятии неважное: прибыли нет, большая текучесть кадров.

Руководство холдинга поручило СКР разобраться с положением, защитить интересы фирмы, обеспечить безопасность персонала.

**ВОПРОС:**

При отработке версий и выполнении задания к кому необходимо было бы обратиться за помощью и какие вопросы решать?

**ЗАДАЧА 5.**

Торговая компания г. Томска закупила в Москве партию изделий бытовой электроники общим объемом около 5 грузовых автомобилей. По условиям контракта товар продавался со склада в Москве, далее самовывозом. Полную партию товара продавец обязался поставить в течение недели частями.

Покупатель решил везти груз на автомобилях, арендованных в Московских транспортных агентствах.

Охрану груза было поручено осуществлять СБ компании.

**ВОПРОС:**

Какие меры следует предпринять СБ компании для обеспечения сохранности груза?

**ЗАДАЧА 6.**

Коммерческий банк «Развитие» по личной рекомендации Председателя союза банков принял в качестве клиента ТОО «Веста», где учредителями были российская гражданка и турецкий гражданин. Через некоторое время турок объявил, что готовит очень крупный контракт по строительству индивидуальных коттеджей и попросил кредит на 40 млн. рублей. Так как в

залог он представить ничего не мог, за него выступил с ходатайством «по дружбе» Председатель союза. Еще через некоторое время он попросил кредит на 80 млн. руб. и в качестве залога предложил арендный договор на землю. Получив кредиты, турок перестал вести расчеты через этот банк и вскоре объявил о закрытии фирмы.

Предварительным расследованием СКР банка установлено, что кредит турок использовал на другие нужды. Денег на счету новой фирмы почти нет. Арендный договор на землю был оформлен с грубейшими нарушениями закона в сговоре с председателем колхоза. В финансовых документах отмечается умышленное искажение отчетности, налоги нс платились. Существенную поддержку турку оказывал бывший руководящий сотрудник правоохранительного министерства.

**ВОПРОСЫ:**

- 1. Какие предупредительные меры нужно было предпринять СКР в отношении гражданина Турции?
- 2. По каким направлениям следует вести разработку турка, чтобы поставить его перед необходимостью вернуть взятый кредит?

## 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Информационно-аналитические системы безопасности» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета

| Неделя текущего контроля | Вид оценочного средства | Код компетенций, оценивающий знания, умения, навыки | Содержание оценочного средства | Требования к выполнению | Срок сдачи (неделя семестра) | Критерии оценки по содержанию и качеству с указанием баллов |
|---|---|---|---|---|---|---|
| *Проводится в сроки, установленные графиком образовательного процесса* | тестирование | ПК-1; ПК-3 | 20 вопросов | Компьютерное тестирование ; время отведенное на процедуру - 30 минут | Результаты тестирования предоставляются в день проведения процедуры | *Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.* |
| *Проводится в сроки, установленные графиком образовательного процесса* | тестирование | ПК-1; ПК-3 | 20 вопросов | Компьютерное тестирование; время отведенное на процедуру – 30 минут | Результаты тестирования предоставляются в день проведения процедуры | *Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.* |
| *Проводится в сроки, установленные графиком образовательного процесса* | Зачет | ПК-1; ПК-3 | 3 вопроса | Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут. | Результаты предоставляются в день проведения зачета | *Критерии оценки: **«Зачтено»:*** • *знание основных понятий предмета;* • *умение использовать и применять полученные знания на* |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | *практике;*<br>• *работа на семинарских занятиях;*<br>• *знание основных научных теорий, изучаемых предметов;*<br>• *ответ на вопросы билета.*<br>***«Не зачтено»:***<br>*демонстрирует частичные знания по темам дисциплин;*<br>• *незнание основных понятий предмета;*<br>• *неумение использовать и применять полученные знания на практике;*<br>• *не работал на семинарских занятиях;*<br>• *не отвечает на вопросы.* |

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.

### 4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

1. Требование безопасности повторного использования объектов противоречит:
   инкапсуляции
   наследованию
   полиморфизму

2. Предположим, что при разграничении доступа учитывается семантика программ. В таком случае на игровую программу могут быть наложены следующие ограничения:
   запрет на чтение каких-либо файлов, кроме конфигурационных
   запрет на изменение каких-либо файлов, кроме конфигурационных
   запрет на установление сетевых соединений

3. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
   меры обеспечения целостности
   административные меры
   меры административного воздействия

4. Дублирование сообщений является угрозой:
   доступности
   конфиденциальности
   целостности

5. Самыми опасными источниками внутренних угроз являются:
   некомпетентные руководители
   обиженные сотрудники
   любопытные администраторы

6. Для внедрения бомб чаще всего используются ошибки типа:
   отсутствие проверок кодов возврата
   переполнение буфера
   нарушение целостности транзакций

7. В число целей политики безопасности верхнего уровня входят:
   решение сформировать или пересмотреть комплексную программу безопасности
   обеспечение базы для соблюдения законов и правил
   обеспечение конфиденциальности почтовых сообщений

8. В число целей программы безопасности верхнего уровня входят:
   управление рисками

определение ответственных за информационные сервисы
определение мер наказания за нарушения политики безопасности

9. В рамках программы безопасности нижнего уровня осуществляются:
стратегическое планирование
повседневное администрирование
отслеживание слабых мест защиты

10. Политика безопасности строится на основе:
общих представлений об ИС организации
изучения политик родственных организаций
анализа рисков

11. В число целей политики безопасности верхнего уровня входят:
формулировка административных решений по важнейшим аспектам реализации программы безопасности
выбор методов аутентификации пользователей
обеспечение базы для соблюдения законов и правил

## 4.2.Типовые вопросы, выносимые на зачет

1. Информационно – аналитическое обеспечение деятельности органов власти. Общие подходы.
2. Специфика принятия решений в органах управления и основные проблемы создания комплексных систем информационно – аналитического обеспечения деятельности органов власти.
3. Стратегический уровень регионального управления. Оперативное управление. Управление в условиях черезвычайных ситуаций.
4. Требования к работе информационно – аналитических подразделений органов управления.
5. Информационно-аналитическая система поддержки принятия решений руководителем субъекта российской Федерации.
6. Основы построения систем информационно – аналитического обеспечения управления регионом на примере Санкт-Петербурга.
7. Функциональная структура системы информационно – аналитического обеспечения и ее место в управлении регионом.
8. Нормативно – правовое обеспечение работ по подготовке информационно – аналитических материалов.
9. Виды информационно – аналитических материалов и требования к их составу и содержанию.
10. Методология анализа информации при подготовке информационно- аналитических материалов.
11. Применение методов анализа информации и моделирование процессов жизнедеятельности (на основе опыта эксплуатации ИАО)

12. Интерпретация результатов исследуемой проблемы возможным вариантам управленческих решений. Подготовка информационно – аналитических материалов и создание дизайна

13. Общие представления о мониторинге. Стратегический мониторинг. Оперативный мониторинг. Задачи разведывательного мониторинга. Мониторинг средств массовой информации.

14. Мониторинг массовых настроений. Мониторинг массовой активности.

15. Мониторинг учреждений. Мониторинг ведущих деятелей.

16. Системы обнаружения. Системы оперативного информирования. Феномен предсказывания. Возможности предсказывания. Ясновидение.

17. Система прогнозирования. Структура прогноза. Метод имитационного моделирования. Метод Делфи.

18. Метод морфологического анализа. Метод "дерева целей". Неформальное прогнозирование. Думание за противника. Место прогнозирования в системе деятельности.

19. Прогнозирование индивидуума. Прогнозирование массовых настроений. Прогнозирование выборов. Прогнозирование событий.

20. Тактическое прогнозирование. Стратегическое прогнозирование.

21. Поддержка решений. Системы оперативного прогнозирования. Экспертные системы.

22. Системы поддержки нетипового анализа числовых данных. Системы для контент - анализа. Системы для фильтрования данных.

23. Системы поддержки неформального анализа текстов. Базы данных аналитической разведки. Интернет как средство разведки и влияния.

24. Мониторинг в интернете. Направленный поиск в интернете. Управление поиском в интернете.

25. Индивидуальное использование интернета. Поиск в интернете. "Активная" деятельность в интернете. Способы повышения эффективности Личная информационная система. Использование компьютера. Теория влияния.

26. Манипулирование руководителями. Нейтрализация руководителей. Манипулирование массами. Поддержка интеллектуалов. Нейтрализация активистов. Влияние на выборы.

27. Противодействие влиянию на аналитическую разведку. Противодействие влиянию на руководителей. Противодействие влиянию на общество в целом.

28. Логика процесса исследования. Информационная работа. Основные этапы информационно-аналитической работы. Работа с источниками информации.

29. Планирование работы. Начало работы. Способы работы. Поиск информации. Документальные источники информации. Работа с книгой. Техника чтения.

30. Источники информации. Обретение доступа к документам. Перехват и перлюстрация писем.

31. Обработка «мусора». Техника интерпретации данных. Обеспечение безопасности и защиты информации.

32. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность

**Приложение 2**

**Методические указания для обучающихся по освоению дисциплины (модуля)**

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ**

**КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ) ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ БЕЗОПАСНОСТИ

**Направление подготовки: 10.04.01 - Информационная безопасность**

**Направленность (профиль): Менеджмент информационной безопасности**

**Уровень высшего образования: магистратура**

**Форма обучения: очная**

Королев
2023

## 1. Общие положения

**Цель дисциплины:**

**Целью изучения дисциплины является** научить студентов решать задачи связанные с созданием, эксплуатацией, развитием и защитой автоматизированных ИАС, обеспечивающих отработку и анализ специальной информации в процессе информационно – аналитической деятельности в интересах региона

Дать представление об учете и использовании особенностей информационных технологий, применяемых в автоматизированных ИАС, для информационно-аналитического обеспечения мониторинга

Уметь, формировать и реализовывать комплекс мероприятий по защите информации в автоматизированных ИС информационной безопасности.

**Задачи дисциплины:**

- Научить студентов проводить анализ и исследовать модели автоматизированных ИС, обеспечивающих обработку и анализ специальной информации в целях принятия решений в процессе ИА деятельности (специальные ИАС);
- Научить применять на практике стандарты, относящиеся к обеспечению информационной безопасности;
- Проводить синтез и анализ проектных решений по ИА обеспечению информационной безопасности;
- Обеспечить эффективное применение информационно-технологических ресурсов с учетом нормативных требований по защите информации;
- Разрабатывать и реализовывать политики информационной безопасности для ИАС различно назначения;
- Участвовать в проектировании и эксплуатации системы управления информационной безопасностью;
- Разрабатывать предложения по совершенствованию системы управления информационной безопасностью;
- Формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной АИС;
- Применять модели, методы и методики информационно – аналитической деятельности, реализуемые с применением ИАС.

## 2. Указания по проведению практических занятий

### Тема 1. Информационно – аналитическое обеспечение деятельности информационной безопасности региона

**Практическое занятие 1.**
Вид практического занятия: смешанная форма практического занятия.
Образовательные технологии: *практическая работа в группах*
Тема и содержание практического занятия:
Цель работы: Получить практические знания об общих подходах информационно аналитического обеспечения деятельности органов власти.
Учебные вопросы:
- Общие подходы.
- Специфика принятия решений в органах управления.
- основные проблемы создания комплексных систем информационно – аналитического обеспечения деятельности органов власти.

Продолжительность занятия -4 часа.

### Тема 2. Особенности организации регионального управления информационной безопасностью (требования к работе информационно – аналитических подразделений)

**Практическое занятие 2**.
Вид практического занятия: смешанная форма практического занятия.
Образовательные технологии: *групповая дискуссия.*
Тема и содержание практического занятия:
Цель работы: Получить практические знания и навыки о политике безопасности отдельных структур
Учебные вопросы:
- Оперативное управление
- Управление в условиях чрезвычайных ситуаций
- Требования к работе информационно – аналитических подразделений органов управления

Продолжительность занятия -4 часа.

## Раздел 2. Прикладные аспекты управления информационной безопасностью

### Тема 3. Основы построения систем информационно – аналитического обеспечения управления безопасностью в органах государственной власти и местного самоуправления региона

**Практическое занятие 3.**
Вид практического занятия: смешанная форма практического занятия.

Образовательные технологии: *подготовка реферата*
Тема и содержание практического занятия:
Цель работы: Получить практические знания и навыки в организационно-кадровых и технических аспектах управления информационной безопасностью
Учебные вопросы:
- Основы построения систем информационно – аналитического обеспечения управления регионом
- Функциональная структура системы информационно – аналитического обеспечения
- Место системы информационно – аналитического обеспечения в управлении регионом

Продолжительность занятия -4 часа.

**Тема 4. Инструментарий информационно – аналитической поддержки принятия решений в органах государственной власти и местного самоуправления региона**

**Практическое занятие 4.**
Вид практического занятия: смешанная форма практического занятия.
Образовательные технологии: *групповая дискуссия.*
Тема и содержание практического занятия:
Цель работы: Получить практические знания и навыки оценки эффективности управления ИБ
Учебные вопросы:
- Нормативно – правовое обеспечение работ по подготовке информационно – аналитических материалов
- Виды информационно – аналитических материалов
- Требования к видам информационно – аналитических материалов составу и содержанию

Продолжительность занятия -4 часа.

## 3. Указания по проведению лабораторного практикума

*Цель и задачи выполнения лабораторных работ:* Определение порядка и последовательности действий по обоснованию предложений руководителю по результатам анализа и прогноза по заданной ситуации.

Методика *определяется моделью соответствующей задачи, решаемой обучающимся на занятии по заданию преподавателя)* и средства *для* выполнения лабораторных работ: общее *программное обеспечение*

Этапы выполнения лабораторных работ *(Постановка задачи лабораторной работы. Ознакомление обучающегося с содержанием и объемом лабораторной работы. Порядок выполнения лабораторной*

*работы. Регистрация результатов и оформление отчета о лабораторной работе. Заключительная часть лабораторной работы).*

Тематика лабораторных работ и задания к ним *(тематика лабораторных работ должна соответствовать рабочей программе дисциплины).*

**Лабораторная работа № 1.**

**Тема: Структура информационных ресурсов и администрирование в компьютерных системах**

Цель занятия: Определение конфигурации информационных ресурсов компьютерных систем. Администрирование в компьютерных системах.

Продолжительность практического занятия-2 часа

Задание.

Агропромышленная фирма «Юниор» имеет головное предприятие в Москве и несколько дочерних фирм в различных регионах России. К руководству фирмы «Юниор» на одной специализированной выставке обратился господин N, представившийся сотрудником известной зарубежной компании «АВС», с предложением об участии в совместном проекте в регионе, в котором «Юниор» имеет дочернюю фирму.

**ВОПРОСЫ:**

- 1. Какие мероприятия по проверке потенциального зарубежного партнера компании «АВС» должна провести Служба Конкурентной Разведки фирмы «Юниор»?
- 2. На какие моменты необходимо обратить особое внимание?

**Лабораторная работа № 2.**

**Тема: Анализ угроз информационной безопасности**

Цель занятия: Факторы, воздействующие на защищаемую информацию. Классификация угроз. Естественные и искусственные угрозы. Основные направления и методы реализации угроз.

Основные виды атак на КС, их классификация. Проблемы обеспечения информационной безопасности в проводных КС.

Беспроводной доступ к локальным сетям. Угрозы и уязвимости в беспроводных компьютерных системах.

Продолжительность практического занятия-2 часа

Задание.

Фармацевтическая компания «Иванов и сын» разработала и запатентовала уникальный лекарственный препарат. Важнейшим компонентом этого препарата является сырье, ввозимое из-за рубежа (в мире имеется всего несколько поставщиков этого сырья). Руководство компании

планирует выйти на рынок лекарственных препаратов аналогичного класса и поручает службе безопасности провести анализ конкурентной среды.

**ВОПРОСЫ:**

- 1. Какой метод анализа следует применить для решения этой задачи?
- 2. Предложить методику проведения анализа. Какая, на ваш взгляд, наиболее опасная внешняя угроза существует для этой фирмы?

**Лабораторная работа № 3.**
**Тема: Основные уровни защиты информации в компьютерных системах**
Цель занятия: Методы и средства обеспечения защиты информации в компьютерных системах. Защита представления информации. Защита содержания информации.
Сертификация программных и программно-технических средств защиты конфиденциальной компьютерной информации.
Методы обеспечения защиты информации – препятствие, маскировка, управление доступом. Функции защиты при управлении доступом. Принуждение и побуждение.
Физические средства защиты компьютерных систем. Нейтрализация утечки информации по электромагнитным каналам – применение генераторов шума. Защита от наводок. Аппаратные средства защиты в КС. Задачи, решаемые программными средствами защиты.
Продолжительность практического занятия-2 часа
Задание.

Российская транспортная компания «Зевс» осуществляет грузоперевозки элементов мебели (мебельный щит, гнутые детали и т.д.) на мебельные фабрики конкурирующих фирм «Альт» (Германия) и «Вист» (Италия). Представители фирмы «Альт» пытаются получить конфиденциальную информацию у служащих фирмы «Зевс» об объемах поставок фирмы «Вист», графике движений, реквизитах грузов, стоимости транспортных услуг и т.д.

**ВОПРОСЫ:**

1. Какими методами компания «Альт» может получить необходимую ей конфиденциальную информацию?

2.Какие меры должна предпринять компания «Вист» для защиты собственной конфиденциальной информации?

**Лабораторная работа № 4.**
**Тема: Основные положения формальной теории защиты информации**

Цель занятия: Концепция монитора безопасности обращений в КС.
Правила разграничения доступа субъектов к объектам в ОС.
Монитор безопасности обращений (МБО) субъектов к объектам. Схема монитора безопасности обращений. Функции МБО. Свойства МБО
Продолжительность практического занятия-2 часа
Задание.

Малое предприятие «Электрон», занимающееся разработкой программных продуктов, успешно конкурирует с зарубежной фирмой «Гейтсан». Успех «Электрона» во многом связан с группой (из 3 человек) высококвалифицированных программистов.

**ВОПРОСЫ:**

- 1. Какие шаги может предпринять фирма «Гейтсан» для вытеснения фирмы «Электрон» с рынка?
- 2. Какие индикаторы (внешние проявления) могут служить сигналами о начале наступления «Гейтсана»?
- 3. На что должны быть направлены действия Службы Конкурентной Разведки фирмы «Электрон» для защиты интересов своей фирмы?

## 4. Указания по проведению самостоятельной работы студентов

| № п/п | Наименование блока (раздела) дисциплины | Виды СРС |
|---|---|---|
| 1. | Информационно – аналитическое обеспечение деятельности информационной безопасности региона | ***Подготовка докладов по темам:***<br>Место информационной безопасности в системе национальной безопасности.<br>Современная концепция информационной безопасности.<br>Цели и концептуальные основы защиты информации.<br>***Самостоятельное изучение темы*** (тематика определяется преподавателем |
| 2. | Особенности организации регионального управления информационной безопасностью (требования к работе информационно – аналитических подразделений) | ***Подготовка докладов по темам:***<br><br>Критерии, условия и принципы отнесения информации к защищаемой.<br>Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.<br>Понятие и структура угроз защищаемой информации. |
| 3 | Основы построения систем информационно – аналитического | ***Подготовка докладов по темам:***<br>Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию.<br>Причины, обстоятельства и условия, вызывающие |

| | | |
|---|---|---|
| | обеспечения управления безопасностью в органах государственной власти и местного самоуправления региона | дестабилизирующее воздействие на защищаемую информацию.<br>Виды уязвимости информации и формы ее проявления.<br>***Самостоятельное изучение темы*** (тематика определяется преподавателем |
| 4 | Инструментарий информационно – аналитической поддержки принятия решений в органах государственной власти и местного самоуправления региона | ***Подготовка докладов по темам:***<br>Критерии оценки безопасности информационных технологий.<br>Методы защиты информации от несанкционированного доступа.<br>Риски информационной безопасности.<br>***Самостоятельное изучение темы*** (тематика определяется преподавателем<br>**Письменная работа**<br>Предложения руководителю для принятия решения в рамках ИАД по обеспечению безопасности функционирования объекта информатизации. |

## 5. Указания по проведению контрольных работ для обучающихся очной формы обучения

### 5.1. Требования к структуре.

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

### 5.2. Требования к содержанию (основной части).

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.
2. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы: «раскрыть», «определить», «установить», «показать», «выявить» и т.д.
3. Основная часть работы включает 2 - 4 вопроса, каждый из которых посвящается решению задач, сформулированных во введении, и заканчивается констатацией итогов.
4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).
5. Необходимо давать ссылки на используемую литературу.
6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.
7. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями. Если в

работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

**5.3. Требования к оформлению.**

Объём контрольной работы – **…** страниц формата А4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

## 6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

**Основная литература:**

**1.** Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: https://doi.org/10.29039/01848-4. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232287 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

2. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

**Дополнительная литература:**

1. Коноплева, И. А. Управление безопасностью и безопасность бизнеса : учебное пособие для вузов / И. А. Коноплева, И. А. Богданов ; под ред. И. А. Коноплевой. — Москва : ИНФРА-М, 2020. — 448 с. — (Высшее образование). - ISBN 978-5-16-003230-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1068834 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

2. Федотова, Е. Л. Информационные технологии и системы : учебное пособие / Е. Л. Федотова. — Москва : ФОРУМ : ИНФРА-М, 2022. — 352 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0927-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1839925 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

**3.** Меняев, М. Ф. Цифровая экономика предприятия : учебник / М.Ф. Меняев. — Москва : ИНФРА-М, 2021. — 369 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1045031. - ISBN 978-5-16-015656-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1217285 (дата обращения: 03.10.2022). – Режим доступа: по подписке.

**7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)**

**Интернет-ресурсы**:

1. www.biblioclub.ru - Универсальная библиотека онлайн.
2. www.rucont.ru - ЭБС «Руконт».
3. http://www.academy.it.ru/ – академия АЙТИ.
4. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
5. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации
6. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности
7. http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

**8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)**

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**

1. Электронные ресурсы образовательной среды Университета.
2. Информационно-справочные системы: Консультант+; Гарант.