



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

«УТВЕРЖДАЮ»

И.о. проректора

А.В. Троицкий

« » 2023 г.

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И
ТЕХНОЛОГИЙ**

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ (МОДУЛЯ)

Б.1.В.01.04 «ОСНОВЫ КОНКУРЕНТНОЙ РАЗВЕДКИ»

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

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: «Основы конкурентной разведки». – Королев МО: «Технологический университет», 2023.

Рецензент: **Соляной В.Н.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.03.01 «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)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переподтверждения)	2023	2024	2025	2026
Номер и дата протокола заседания кафедры	№ 8 от 29.03.2023			

Рабочая программа согласована:

Руководитель ОПОП ВО

 Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переподтверждения)	2023	2024	2025	2026
Номер и дата протокола заседания УМС	№ 5 от 11.04.2023			

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП

Целями изучения дисциплины является:

Получение обучаемым достаточно полное представление о развитии понятий «информации», «информационная работа» и «аналитическая работа», целях, задачах, методах планирования информационно-аналитической работы, роли информационно-аналитической работы в обнаружении каналов несанкционированного доступа к конфиденциальной информации и, в целом, для обеспечения комплексной безопасности предприятия.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;

ПК-4 Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций

Основными задачами дисциплины являются:

1. Определение основных понятий, связанных с организацией информационно-аналитической деятельностью при обеспечении информационной безопасности на современных предприятиях;

2. Раскрытие базовых составляющих информационно-аналитической деятельности по обеспечению комплексной безопасности;

3. Ознакомление с основными подходами реализации информационно-аналитической деятельности в сфере информационной безопасности в государственных и коммерческих организациях;

4. Раскрытие базового уровня нормативно-законодательных и административно-технических мер информационно-аналитической деятельности по обеспечению комплексной безопасности;

5. Ознакомление с практическими вопросами по использованию современных технологий и средств информационно-аналитической деятельности при обеспечении информационной безопасности на предприятии.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- формулирование цели, задач, значимости, ожидаемых результатов проекта

- знать нормативно-методические, руководящие и методические документы, организационные меры, критерии оценки защищенности и регламенты обеспечения работоспособности систем ЗИ;

Необходимые умения:

- определение потребности в ресурсах для реализации проекта
- определять и оценивать источники, причины и последствия возникающих инцидентов выявлять и устранять нарушения в области ИБ (ЗИ);

Трудовые действия:

- оценка эффективности реализации проекта и разработка плана действий по его корректировке.
- разработка плана реализации проекта
- контроль реализации проекта
- принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Основы конкурентной разведки» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Нормативные акты и стандарты по информационной безопасности», «Информационные процессы и системы как объекты информационной безопасности», «Информационные технологии» и компетенциях: ОК-4,5, ОПК-2,3,4,5,7, ПК-2,3,5,6,8,10,13,15 и ПСК-2.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

Таблица 1

Виды занятий	Всего часов	Семестр 3	Семестр 4	Семестр 5	Семестр 6
Общая трудоемкость	144	72	72		
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	32	16	16		
Лекции (Л)	-	-			
Практические занятия (ПЗ)	32	16	16		
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	92	46	46		
Другие виды контактной работы	20	10	10		
Практическая подготовка	Нет	-	-		
Курсовые работы (проекты)	-	-	-		
Расчетно-графические работы	-	-	-		
Контрольная работа, домашнее задание	+ -	+ -	+		
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	T1; T2	T1; T2	T1; T2		
Вид итогового контроля	Зачет	Зачет	Зачет с оценкой		
ОЧНО - ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	32			16	16
Лекции (Л)	16			8	8
Практические занятия (ПЗ)	16			8	8
Лабораторные работы (ЛР)	-				
Самостоятельная работа	112			66	66
Курсовые работы (проекты)	-			-	-
Расчетно-графические работы	-			-	-
Контрольная работа, домашнее задание	+ -			+	+
Другие виды контактной работы	20			10	10
Практическая подготовка	нет				
Вид итогового контроля	Зачет/ Зачет с оценкой			Зачет	Зачет с оценкой

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

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное/очно-заочное	Практические занятия, час Очное/очно-заочное	Занятия в интерактивной форме, час	Код компетенций
Раздел (модуль) 1. Содержание информационно-аналитической деятельности				
Тема 1. Базовые положения по информационно-аналитической деятельности	-/1	5/1	1/1	УК-2; ПК-4
Тема 2. Основы информационно-аналитической деятельности при обеспечении информационной безопасности	-/3	6/3	1/1	УК-2; ПК-4
Раздел (модуль) 2. Организация информационно-аналитической деятельности				
Тема 3. Методика информационно-аналитической работы	-/3	6/3	1/1	УК-2; ПК-4
Тема 4. Методы изучения документальных источников	-/3	4/3	1/1	УК-2; ПК-4
Тема 5. Формы и виды составления отчетов о проделанной информационно-аналитической работе	-/3	4/3	2/2	УК-2; ПК-4
Итого:	-/16	32/16	6/6	

4.2. Содержание тем дисциплины

Раздел (модуль) №1

Содержание информационно-аналитической деятельности Тема 1. Базовые положения по информационно-аналитической деятельности

Информационная работа как вид деятельности, включающий в качестве составляющих элементов, добывание, накопление, обработку, хранение и выдачу информации.

Понятие аналитическая работа. Аналитическая работа как вид деятельности направленный на получение ценной информации о конкурентах, новизне их продукции и разрабатываемых новшествах. Содержание аналитической работы.

Субъекты и объекты информационно-аналитической работы. Принципы информационно-аналитической работы. Направления и основные этапы информационно-аналитической работы.

Тема 2. Основы информационно-аналитической деятельности при обеспечении информационной безопасности

Информационно-аналитическая деятельность в службе информационной безопасности предприятия. Информационно-аналитическое подразделение: цели, задачи, функции.

Информационно-аналитическая деятельность в сфере управления информационной безопасностью. Структура организации и методика отбора сотрудников для создания рабочих информационно-аналитических групп.

Роль информационно-аналитической работы в обнаружении каналов несанкционированного доступа к информации фирмы.

Раздел (модуль) №2.

Организация информационно-аналитической деятельности

Тема 3. Методика информационно-аналитической работы

Алгоритм информационно-аналитической деятельности: общее ознакомление с проблемой; определение ее внешних границ; формулирование цели деятельности; постановка задач на проведение аналитических работ; разработка целесообразного варианта проведения информационно-аналитической деятельности; реализация принятого варианта аналитических работ; обобщение и синтез полученных аналитических данных.

Тема 4. Методы изучения документальных источников

Классификация источников. Эксперт. Внутренний информатор (осведомитель). «Горячий» информатор. Внедренный источник. Легкомысленный информатор («болтун»). Контактеры. Союзник. Случайный источник.

Официальные документы. Деловые бумаги и архивы. Носители машинной информации. Личные бумаги и архивы. «Мусор». Обнародованные сведения. Подметные письма и самиздат.

Понятие открытой (более или менее доступной); полужакрытой (не засекреченной, но контролируемой теми, кого она касается); секретной информации.

Пути получения информации: изъятие, перфорация, ксерокопирование, фотографирование и др.

Выявление источников информации. Организация справочно-информационной деятельности. Последовательность поиска документальных источников информации. Планирование работы. Этапы и процессы аналитической работы. Этапы и процессы информационной работы. Организация справочно-информационной деятельности.

Органы научно-технической информации. Последовательность поиска документальных источников информации. Методы анализа документов: исторический метод; метод внешней и внутренней критики; социологический метод; контентный анализ; статистический; лингвистический; морфологический и социологический анализ.

Принципы и критерии оценки и анализа информации. Достоверность и надежность материалов. Искажение информации и дезинформация. Техника интерпретации данных.

Тема 5. Формы и виды составления отчетов о проделанной информационно-аналитической работе

Формы предоставления отчета: письменный, устный иллюстрируемый отчет, устный отчет.

Тактический отчет (оперативный отчет). Методика и форма составления.

Стратегический отчет. Методика и форма составления. Периодический отчет. Методика и форма составления.

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-аналитическая деятельность по обеспечению комплексной 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:

3. 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.
4. 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.
5. 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.
6. С. И. Журин. Практика и теория использования детекторов лжи /- 2-е пзд., стереотип. - М.: Горячая линия-Телеком, 2011.
- Белый В.М. Теория информационного менеджмента. Монография. Королев: «Канцлер», 2010.
7. А.А. Демидов, Ю.Н. Захаров. Информационно – аналитические системы принятия решений в органах государственной власти и местного самоуправления. Основы проектирования и внедрения. Учебное пособие. СПб: НИУ ИТМО, 2012.-100 с.
8. Д. В. Исаев. Аналитические информационные системы. Учебное пособие. ГУ ВШЭ.- М., 2008. - 60 с.
- Л. А. Демидова. Принятие решений в условиях неопределенности /, В. В. Кираковский. А. Н. Пылькин. - М.: Горячая линия — ТВДИЖОМ, 2012.-288 с: ил.
9. Васильков А.В. Информационные системы и их безопасность. Учебное пособие.- М.: ФОРУМ, 2010.
10. А.Ф. Чипига. Информационная безопасность автоматизированных систем. Учебное пособие.- Гелиос АРВ, 2010.

11. Гамза В.А., Ткачук И.Б. Безопасность банковской деятельности: учебник.- 2 –е изд., перераб. и доп. – М.: Маркет ДС, 2010.-408 с. (Универсететская серия).

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

Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал
2. <http://informika.ru/> – образовательный портал
3. <http://www.academy.it.ru/> – академия АЙТИ
4. www.wikIsec.ru - Энциклопедия информационной безопасности -

Публикации, статьи

5. www.biblioclub.ru - Универсальная библиотека онлайн
6. www.rucont.ru - ЭБС «Рукопт»
7. <http://www.minfin.ru> - Официальный сайт Министерства финансов Российской Федерации
8. <http://www.gov.ru/> - Официальный сервер органов государственной власти Российской Федерации
9. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности
10. <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, PowerPoint.

Информационные справочные системы:

Ресурсы информационно-образовательной среды МГОТУ.

Информационно-справочные системы (Консультант+, Гарант.)

Рабочая программа и методическое обеспечение по курсу: «Основы конкурентной разведки»

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.

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И
ТЕХНОЛОГИЙ**

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО
ДИСЦИПЛИНЕ**

«ОСНОВЫ КОНКУРЕНТНОЙ РАЗВЕДКИ»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

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

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;	Тема:1,3,4,5	<ul style="list-style-type: none"> - оценка эффективности реализации проекта и разработка плана действий по его корректировке. - разработка плана реализации проекта - контроль реализации проекта 	<ul style="list-style-type: none"> - определение потребности в ресурсах для реализации проекта 	<ul style="list-style-type: none"> - формулирование цели, задач, значимости, ожидаемых результатов проекта
2.	ПК-4	Способность осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций	Тема 1-5	<ul style="list-style-type: none"> - принимать участие в организации и проведении контрольных проверок работоспособности и эффективности 	<ul style="list-style-type: none"> - определять и оценивать источники, причины и последствия возникающих инцидентов выявлять и устранять нарушения в области ИБ (ЗИ); 	<ul style="list-style-type: none"> - знать нормативно-методические, руководящие и методические документы, организационные меры, критерии оценки защищенности и регламенты обеспечения работоспособности

				применяем ых программн ых, программн о- аппаратны х и технически х средств защиты информаци и;		ти систем ЗИ;
--	--	--	--	--	--	---------------

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

Код компетенции	Инструмент, оценивающий сформированность компетенции	Этапы и показатель оценивания компетенции	Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания
УК-2; ПК-4	<i>Доклад</i>	<p><i>А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов</i></p> <p><i>Б) частично сформирована:</i></p> <ul style="list-style-type: none"> <i>• компетенция освоена на <u>продвинутом</u> уровне – 4 балла;</i> <i>• компетенция освоена на <u>базовом</u> уровне – 3 балла;</i> <p><i>В) не сформирована (компетенция <u>не сформирована</u>) – 2 и менее баллов</i></p> 	<p><i>Например:</i> <i>Проводится в письменной и/или устной форме.</i> <i>Критерии оценки:</i></p> <ol style="list-style-type: none"> <i>1. Соответствие содержания доклада заявленной тематике (1 балл).</i> <i>2. Качество источников и их количество при подготовке работы (1 балл).</i> <i>3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).</i> <i>4. Качество самой представленной работы (1 балл).</i> <i>5. Оригинальность подхода и всестороннее раскрытие выбранной тематике (1 балл).</i> <p><i>Максимальная сумма баллов - 5 баллов.</i></p>
УК-2; ПК-4	<i>Выполнение контрольной работы</i>	<p><i>А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов</i></p> <p><i>Б) частично сформирована:</i></p> <ul style="list-style-type: none"> <i>• компетенция освоена на <u>продвинутом</u> уровне – 4 балла;</i> <i>• компетенция освоена на <u>базовом</u> уровне – 3 балла;</i> <p><i>В) не сформирована (компетенция <u>не сформирована</u>) – 2 и менее баллов</i></p> 	<p><i>При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида</i></p>

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 презентационной форме:

1. Информационно - аналитическая деятельность в органах государственной власти.
2. Методика информационно-аналитической работы
3. Основные этапы информационно аналитической деятельности
4. Информационно-аналитическое подразделение: цели, задачи, функции.
5. Форма и виды отчета о проделанной информационно-аналитической работе.
6. Вопросы организации информационно-аналитической деятельности. Средства аналитической работы, приводящих к достижению целей и задач исследования.
7. Технология аналитической работы.
8. Источники поступления информации в информационно-аналитической работе.
9. Понятия «информация», «информационно-аналитическая работа» в сфере управления, информационно-аналитическая работа (иар) с документами.
10. Содержание информационной работы.
11. Цели и задачи информационной работы.
12. Планирование информационно-аналитической работы.
13. Понятие аналитической работы.
14. Предмет, формы аналитической работы.

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

Формой контроля знаний по дисциплине «Информационно-аналитическая деятельность по обеспечению комплексной безопасности» являются две текущие аттестации в виде тестов и итоговая аттестация в виде экзамена.

Неделя текущего контроля	Вид оценочного средства	Код компетенции, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
--------------------------	-------------------------	---	--------------------------------	-------------------------	------------------------------	---

<p><i>Проводится в сроки, установленные графиком образовательного процесса</i></p>	<p>тестирование</p>	<p>УК-2; ПК-4</p>	<p>20 вопросов</p>	<p>Компьютерное тестирование ; время отведенное на процедуру - 30 минут</p>	<p>Результаты тестирования предоставляются в день проведения процедуры</p>	<p>Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов. Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.</p>
<p><i>Проводится в сроки, установленные графиком образовательного процесса</i></p>	<p>тестирование</p>	<p>УК-2; ПК-4</p>	<p>20 вопросов</p>	<p>Компьютерное тестирование; время отведенное на процедуру – 30 минут</p>	<p>Результаты тестирования предоставляются в день проведения процедуры</p>	<p>Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов. Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.</p>
<p><i>Проводится в сроки, установленные графиком образовательного процесса</i></p>	<p>Зачет/зачет с оценкой</p>	<p>УК-2; ПК-4</p>	<p>2 вопроса</p>	<p>Зачет проводится в устной форме, путем ответа на вопросы. Время отведенное на процедуру – 20 минут.</p>	<p>Результаты предоставляются в день проведения зачета</p>	<p>Критерии оценки: «Зачтено»:</p> <ul style="list-style-type: none"> • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на семинарских занятиях; • знание основных научных теорий, изучаемых

						<ul style="list-style-type: none"> • предметов; • ответ на вопросы билета. <p>«Не зачтено»:</p> <ul style="list-style-type: none"> • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на семинарских занятиях; • не отвечает на вопросы.
		<p>2 теоретических вопроса + практическое задание</p>	<p>экзамен проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.</p>	<p>Результаты предоставляются в день проведения экзамена</p>	<p>Критерии оценки:</p> <p>«Отлично»:</p> <ul style="list-style-type: none"> • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. <p>«Хорошо»:</p> <ul style="list-style-type: none"> • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных 	<p>«Хорошо»:</p> <ul style="list-style-type: none"> • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных

					<p>теорий, изучаемых предметов;</p> <ul style="list-style-type: none"> • ответы на вопросы билета • неправильно решено практическое задание <p>«Удовлетворительно»:</p> <ul style="list-style-type: none"> • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; <p>«Неудовлетворительно»:</p> <ul style="list-style-type: none"> • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.
--	--	--	--	--	--

Примерное содержание тестов для текущей аттестации:

ЗАДАНИЕ НА ВЫБОР ОДНОГО ПРАВИЛЬНОГО ВАРИАНТА ОТВЕТА

1. Документирование информации как способ ее сохранения и передачи во времени и пространстве.
2. Информационные процессы: создание, сбор, хранение, поиск,

преобразование информации.

3. Информационно-документационное обслуживание.

4. Понятия «информация», «информационно-аналитическая работа» в сфере управления, информационно-аналитическая работа (ИАР) с документами.

5. Содержание и задачи информационно-аналитической работы (ИАР).

6. Методы обработки информации, применяемые в управлении предприятием.

7. Вопросы организации информационно-аналитической деятельности и работы службы безопасности.

8. Документирование информации как способ ее сохранения и передачи во времени и пространстве.

9. Информационные процессы: создание, сбор, хранение, поиск, преобразование информации.

10. Правовое регулирование информационной сферы в РФ.

11. Понятие, объект, субъект информационно-аналитической работы.

12. Принципы информационно-аналитической работы.

13. Направления ИАР информационно-аналитической работы по обеспечению безопасности фирмы.

14. Вопросы организации информационно-аналитической деятельности.

15. Средства аналитической работы, приводящих к достижению целей и задач исследования. Технология аналитической работы.

16. Источники поступления информации в информационно-аналитической работе.

17. Источники и работа с ними.

18. Критерии оценки информационного материала.

19. Понятие об информационной работе.

20. Содержание информационной работы.

21. Цели и задачи информационной работы.

22. Планирование информационно-аналитической работы.

23. Понятие аналитической работы.

24. Предмет, формы аналитической работы.

25. Этапы и процесс АР.

26. Методы анализа документов при информационно-аналитической работе.

27. Роль ИАР в обнаружении каналов несанкционированного доступа к информации фирмы.

28. Форма и виды отчета о проделанной информационно-аналитической работе.

1. Федеральный государственный контроль за обеспечением защиты государственной осуществляется в порядке, установленном Постановлением Правительства РФ №...

(!) № 1205;

(?) № 1305;

(?) № 205;

(?) № 407.

2. Межведомственный контроль за обеспечением защиты государственной тайны в органах государственной власти осуществляют:

- (!) ФСБ, МО, СВР, ФСТЭК;
- (?) ФСБ, МО, МВД;
- (?) МО, МИД, ФСТЭК;
- (?) ФСБ, ФСО, МВК.

3. ФЗ №114 статья 115: «... при допуске к сведениям особой важности или совершенно секретным выезд из РФ может быть ограничен не более, чем на ...»

- (!) 5 лет;
- (?) 2 года;
- (?) 10 лет;
- (?) 15 лет.

4. Незаконное получение сведений, содержащих государственную тайну, наказывается штрафом в размере ...

- (!) от 200 000 до 500 000 рублей;
- (?) от 400 000 до 700 000 рублей;
- (?) от 500 000 до 1 000 000 рублей;
- (?) от 100 000 до 200 000 рублей.

5. Утрата документов, содержащих государственную тайну, наказывается ограничением свободы на срок до ... лет, либо арестом на срок от ... до ... месяцев.

- (!) 3; 4, 6;
- (?) 5; 6, 12;
- (?) 7; 12,18;
- (?) 10; 18,24.

6. С каким документом тесно связан документ «Критерии Европейской безопасности информационных технологий»

- (?) Конвенция информационной безопасности;
- (?) Закон об информационной защите 1995 г.;
- (!) «Оранжевая книга»;
- (?) Европейская конституция.

7. Что не входит в Функциональные критерии по «Европейским критериям безопасности информационных технологий»

- (?) Аутентификация;
- (?) Конфиденциальность данных;
- (!) Физическая защита здания;
- (?) Целостность данных.

8. Сколько уровней критериев адекватности существует в «Европейских критериях безопасности информационных технологий»

- (?) 3;
- (?) 5;
- (!) 7;
- (?) 8.

9. Сколько классов (шаблонов) в функциональных критериях существует «Европейских критериях безопасности информационных технологий»

- (?) 7;
- (!) 10;
- (?) 7;
- (?) 12.

10. Главное отличие Европейских критериев безопасности от других?

- (!) Не задают шкалу требований и механизмы защиты;
- (?) Связаны только с защитой конфиденциальных данных;
- (?) Требования по защите устанавливаются организацией;
- (?) Действует на все страны мира.

11. Государственную тайну составляют сведения

- (!) В военной области;
- (?) В области учета населения;
- (?) В области образования;
- (?) В области здравоохранения.

12. В соответствии с Федеральным законом РФ «О государственной тайне» основными принципами отнесения информации к государственной тайне являются

- (?) Законность, демократизм и объективизм;
- (!) Законность, обоснованность и современность;
- (?) Законность, демократизм и гуманизм;
- (?) Законность, формализм и объективизм.

13. Какой из типов нормативно-правовых документов регламентирует Информационную безопасность в Российской Федерации?

- (?) Акты федерального законодательства;
- (?) Нормативно-методические документы государственных органов;
- (?) Стандарты информационной безопасности;
- (!) Все выше перечисленные.

14. Отношения, связанные с обработкой персональных данных, регулируются законом

- (?) Об информации, информационных технологиях;
- (?) О защите информации;
- (!) Федеральным законом «О персональных данных»;
- (?) Федеральным законом «О конфиденциальной информации».

15. Информация, доступ к которой ограничивается в соответствии с законодательством РФ

- (?) Персональная информация;
- (?) Информация, составляющая коммерческую тайну;
- (!) Конфиденциальная информация;
- (?) Документированная информация.

16. В каком нормативном акте закреплены все виды конфиденциальной информации?

- (?) В ФЗ-152 «О персональных данных»;
- (!) В Указе Президента №188;
- (?) В Трудовом кодексе РФ;
- (?) В ФЗ-149 «Об информации, информационных технологиях и о защите информации».

17. Какую информацию запрещено относить к конфиденциальной в соответствии с законом РФ?

- (?) Паспортные данные гражданина;
- (!) Информация, накапливаемая в открытых фондах библиотек, музеев, архивов;
- (?) Себестоимость продукта и объем сбыта;
- (?) Контактные данные клиентов.

18. Раскройте понятие «конфиденциальный документ»

- (!) Это зафиксированная на материальном носителе конфиденциальная информация с реквизитами, позволяющими ее идентифицировать;
- (?) Это зафиксированная на материальном носителе конфиденциальная информация с обязательным проставлением грифа конфиденциальности;

(?) Это любая информация имеющая конфиденциальный характер даже если она предоставлена в устном виде;

(?) Все ответы верны.

19. К конфиденциальной информации относятся

(?) Сведения общего доступа, связанные с профессиональной деятельностью;

(!) Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность;

(?) Сведения о кадровом составе, а также системе вознаграждения за проделанную работу;

(?) Сведения о проведении конкурсов, тендеров и прочих мероприятиях, где решается судьба государственной собственности.

20. Отправка конфиденциальных документов осуществляется

(?) Секретарем;

(?) Исполнителем;

(!) Сотрудником службы конфиденциальной информации;

(?) Любой сотрудник.

21. Кто несёт ответственность за классификацию информации?

(?) Руководитель;

(?) Высшее руководство;

(!) Владелец;

(?) Пользователь.

22. Какая категория людей является наиболее опасной для компании с точки зрения вероятности мошенничества и нарушения безопасности?

(!) Сотрудники;

(?) Хакеры;

(?) Атакующие;

(?) Контрагенты (лица, работающие по договору).

23. Что относится к объектам КИИ?

(!) Информационные системы, автоматизированные системы управления технологическим процессом, информационно-телекоммуникационные сети;

(?) ПДН, коммерческая тайна, гос. Тайна;

(?) Системы обработки общедоступной информации.

24. Основной закон для КИИ

(!) Федеральный закон №187;

- (?) Федеральный закон №152;
- (?) Федеральный закон №149;
- (?) Федеральный закон №230.

25. Перечень показателей критериев значимости объекта КИИ определен в ...?

- (!) Постановление Правительства №127;
- (?) Федеральный закон №187;
- (?) ГИС №21;
- (?) ГИС №17.

26. Сколько процентов составляет ежемесячная надбавка к должностному окладу за работу со сведениями, имеющими степень секретности «Совершенно секретно»

- (?) 10-15;
- (!) 30-50;
- (?) 5-10;
- (?) 50-75.

27. Информация о деятельности органов государственной власти и органов местного самоуправления является

- (?) Секретной;
- (?) Особо секретной;
- (!) Открытой;
- (?) Конфиденциальной.

28. Взаимная передача сведений, составляющих государственную тайну, осуществляется

- (?) Юридическими лицами;
- (!) Органами государственной власти;
- (?) Физическими лицами;
- (?) Учреждениями.

29. Степень секретности сведений зависит от

- (?) Степени ущерба, нанесенного конкретным лицам;
- (?) Органов, имеющих эти сведения;
- (!) Тяжести ущерба, который может быть нанесен государству;
- (?) Объема предоставленных сведений.

30. Разглашением государственной тайны является

- (?) Хищение сведений, составляющих гос. тайну;

- (!) Распространение сведений, составляющих гос. тайну;
- (?) Получение сведений, составляющих медицинскую тайну;
- (?) Передача сведений представителями иностранного государства.

31. Одним из принципом политики ИБ является

- (!) Разделение доступа (обязанностей, привилегий) клиентам сети;
- (?) Одноуровневой защиты сети;
- (?) Совместимых, однотипных программно-технических средств сети;
- (?) Многоуровневой защиты.

32. Политика безопасности в системе — это комплекс

- (!) Руководств, требований обеспечения необходимого уровня безопасности;
- (?) Инструкций, алгоритмов поведения пользователя в сети;
- (?) Нормы информационного права, соблюдаемые в сети;
- (?) Рекомендаций.

33. Основным источником права в области обеспечения ИБ в РФ является

- (?) Уголовный кодекс;
- (!) Конституция;
- (?) Государственные и отраслевые стандарты;
- (?) Документы Гостехкомиссии.

34. Система защиты государственной тайны определяется законом

- (?) «Об информации, информатизации и защите информации»;
- (?) «Об органах ФСБ»;
- (!) «О Государственной тайне»;
- (?) «О безопасности».

35. К правовым методам, обеспечивающим ИБ, относятся

- (?) Разработка аппаратных средств обеспечения правовых данных;
- (?) Разработка и установка во всех компьютерных правовых сетях журналов учета действий;
- (!) Разработка и конкретизация правовых нормативных актов обеспечения безопасности;
- (?) Исследования и ликвидация уязвимостей.

36. Одной из целей разработки «Федеральных критериев безопасности информационных технологий» (США) является:

- (!) Определение универсального набора основных требований, предъявляемых к современным информационным технологиям;

- (?) Адаптация результатов новейших исследований в области информационной безопасности;
- (?) Отмена последних изменений в законодательстве;
- (?) Применение опыта европейских коллег к американским реалиям.

37. Какой документ «Федеральных критериев безопасности информационных технологий» (США) был призван заменить?

- (!) Критерии определения безопасности компьютерных систем (Trusted Computer System Evaluation Criteria), так называемая «Оранжевая книга»;
- (?) Критерии компьютерной безопасности (Computer Security Criteria);
- (?) Национальный стандарт безопасности информационных систем (National Information System Security Standard), так называемая «Зелёная книга»;
- (?) Национальные критерии безопасности компьютерных технологий (National Computer Technology Security Criteria).

38. Разработчиками «Федеральных критериев безопасности информационных технологий» (США) выступили:

- (!) NIST и NSA;
- (?) NASA;
- (?) FBI и СВО;
- (?) TSA.

39. В «Федеральных критериев безопасности информационных технологий» (США) под профилем защиты понимается:

- (!) Нормативный документ, регламентирующий требования ко всем аспектам безопасности ИТ-продукта;
- (?) Метод защиты ИТ-продукта;
- (?) Набор технических средств, необходимых для защиты ИТ-продукта от угроз информационной безопасности.

40. Согласно «Федеральных критериев безопасности информационных технологий» (США), разработка профиля защиты осуществляется в

- (!) 3 этапа;
- (?) 2 этапа;
- (?) 4 этапа;
- (?) 6 этапов.

Типовые вопросы, выносимые на экзамен

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

1. Документирование информации как способ ее сохранения и передачи во времени и пространстве.
2. Информационные процессы: создание, сбор, хранение, поиск, преобразование информации.
3. Информационно-документационное обслуживание.
4. Понятия «информация», «информационно-аналитическая работа» в сфере управления, информационно-аналитическая работа (ИАР) с документами.
5. Содержание и задачи информационно-аналитической работы (ИАР).
6. Методы обработки информации, применяемые в управлении предприятием.
7. Вопросы организации информационно-аналитической деятельности и работы службы безопасности.
8. Документирование информации как способ ее сохранения и передачи во времени и пространстве.
9. Информационные процессы: создание, сбор, хранение, поиск, преобразование информации.
10. Правовое регулирование информационной сферы в РФ.
11. Понятие, объект, субъект информационно-аналитической работы.
12. Принципы информационно-аналитической работы.
13. Направления ИАР информационно-аналитической работы по обеспечению безопасности фирмы.
14. Вопросы организации информационно-аналитической деятельности.
15. Средства аналитической работы, приводящих к достижению целей и задач исследования. Технология аналитической работы.
16. Источники поступления информации в информационно-аналитической работе.
17. Источники и работа с ними.
18. Критерии оценки информационного материала.
19. Понятие об информационной работе.
20. Содержание информационной работы.
21. Цели и задачи информационной работы.
22. Планирование информационно-аналитической работы.
23. Понятие аналитической работы.
24. Предмет, формы аналитической работы.
25. Этапы и процесс АР.
26. Методы анализа документов при информационно-аналитической работе.
27. Роль ИАР в обнаружении каналов несанкционированного доступа к информации фирмы.
28. Форма и виды отчета о проделанной информационно-аналитической работе.

ЗАДАНИЕ НА УСТАНОВЛЕНИЕ СООТВЕТСТВИЯ

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. Главным 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, не 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 не 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?

**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.*

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

***ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И
ТЕХНОЛОГИЙ***

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО
ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**

«ОСНОВЫ КОНКУРЕНТНОЙ РАЗВЕДКИ»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

1. Общие положения

Целями изучения дисциплины является:

Получение обучаемым достаточно полное представление о развитии понятий «информации», «информационная работа» и «аналитическая работа», целях, задачах, методах планирования информационно-аналитической работы, роли информационно-аналитической работы в обнаружения каналов несанкционированного доступа к конфиденциальной информации и, в целом, для обеспечения комплексной безопасности предприятия. Сформировать представление о современных методах и средствах информационно-аналитической работы, используемых, в частности, для решения проблем информационной безопасности. Освоение студентами основ информационно-аналитической методов работы.

Задачами дисциплины являются:

1. Определение основных понятий, связанных с организацией информационно-аналитической деятельностью при обеспечении информационной безопасности на современных предприятиях;
2. Раскрытие базовых составляющих информационно-аналитической деятельности по обеспечению комплексной безопасности;
3. Ознакомление с основными подходами реализации информационно-аналитической деятельности в сфере информационной безопасности в государственных и коммерческих организациях;
4. Раскрытие базового уровня нормативно-законодательных и административно-технических мер информационно-аналитической деятельности по обеспечению комплексной безопасности;
5. Ознакомление с практическими вопросами по использованию современных технологий и средств информационно-аналитической деятельности при обеспечении информационной безопасности на предприятии.

2. Указания по проведению практических занятий

Тема 1. Роль и место аналитической разведки в общей системе безопасности. Принципы аналитической разведки

Практическое занятие 1.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Основные положения темы занятия:

- базовые составляющие концепции информационной безопасности информационного объекта.
- основные направления обеспечения информационной безопасности.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Сущность аналитической разведки.
2. Пределы возможностей аналитической разведки.
3. Данные, сведения, информация. Место аналитической разведки.
4. Аналитическая контрразведка. Информационное влияние. Репутация. Конкуренты. Аналитическая разведка и национальная стратегия.
5. Разведка, журналистика, научная деятельность.
6. Разведывательный документ. Искусство сомнения. Обращение внимания на мелочи.
7. Уровни аналитической работы. Феномен истины. Работа с фактами.
8. Обращение с демагогией. Масштабы восприятия. Качество анализа.
9. Аналитическая разведка и официальная идеология. Определение круга интересов. Социальные условия, обеспечивающие эффективность.
10. Использование посторонних специалистов.
11. Стратегия сбора сведений. Специфика аналитической работы. Психогигиена аналитической работы.

Продолжительность занятия- 4.0 /3 часов

**Тема 2. Борьба и обеспечение безопасности в современном обществе. Аналитическая разведка США. Теоретические основания аналитической разведки.
Кадры аналитической разведки**

Практическое занятие 2.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Комплектование. Интеллектуальные качества.
2. Морально-политические качества. Профессиональная подготовка.
3. Развитие аналитических способностей. Формирование коллектива.
4. Человек. Общество. История. Политика. Экономика. Национальная безопасность.
5. Войны. Конфликты. Проблемы. Наука. Теоретизирование. Анализ.

Продолжительность занятия- 4.0 /3 часов

Тема 3. Организация аналитической разведки. Технологии аналитической разведки. Добывание сведений. Обработка сведений. Анализ сведений.

Практическое занятие 3.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Вопросы для обсуждения:

- а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

Структура службы. Размещение службы. Структура деятельности.

Учет работы сотрудников. Защита секретов. Обеспечение эффективности.

Творческие учреждения в системе аналитической разведки.

Компоненты работы. Информационная задача. опережение запросов.

Минимизация ошибок.

Продолжительность занятия- 4.0 /3 часов

Тема 4. Оформление и использование результатов. Задачи разведывательного анализа

Практическое занятие 4.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Структура аналитической записки. Формулирование выводов. Корректность документа. Представление материалов.
2. Анализ текста. Анализ языка. Анализ события. Анализ субъекта. Анализ учреждения. Анализ общественного движения. Анализ деятеля. Анализ публичного заявления. Анализ страны.
3. Выявление заговоров. Выявление агентуры. Выявление намерения начать войну.

Продолжительность занятия- 4.0 /3 часов

Тема 5. Мониторинг. Прогнозирование. Задачи прогнозирования

Практическое занятие 5.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

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

настроений. Прогнозирование выборов. Прогнозирование событий.
Тактическое прогнозирование. Стратегическое прогнозирование.

Продолжительность занятия- 4.0 /3 часов

Тема 6. Технические средства аналитической разведки. Самоорганизация аналитика. Оперативная разведка. Информационное влияние. Противодействие аналитической разведке. Противодействие влиянию.

Практическое занятие 6.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Поддержка решений. Системы оперативного прогнозирования.
2. Экспертные системы. Системы поддержки нетипового анализа числовых данных. Системы для контент - анализа.
3. Системы для фильтрации данных. Системы поддержки неформального анализа текстов. Базы данных аналитической разведки. Интернет как средство разведки и влияния. Мониторинг в интернете.
4. 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.
5. Способы повышения эффективности. Личная информационная система. Использование компьютера. Теория влияния. Манипулирование руководителями.
6. Нейтрализация руководителей. Манипулирование массами. Поддержка интеллектуалов. Нейтрализация активистов. Влияние на выборы.
7. Противодействие влиянию на аналитическую разведку. Противодействие влиянию на руководителей. Противодействие влиянию на общество в целом.

Продолжительность занятия- 4.0 /3 часов

**Тема 7. Методика информационно-аналитической работы.
Содержание информационной и аналитической работы. Работа с
источниками информации**

Практическое занятие 7.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Логика процесса исследования. Методический замысел исследования и его основные этапы. Формулировка гипотезы. Структура и содержание этапов исследовательского процесса.

2. Применение логических законов и правил. Информационная работа. Аналитическая работа. Основные этапы информационно-аналитической работы. Аналогия как метод. От известного к неизвестному. Аналогия.

3. Процентный метод. Аналогия. Характерный пример. Проверка по аналогии. Изучение отдельных случаев как метод информационно-аналитической работы.

4. Планирование работы. Достоинства плана. Начало работы. Способы работы. Запись планов. Ограниченность применения. Поиск информации. Документальные источники информации.

5. Организация справочно-информационной деятельности. Каталоги и картотеки. Библиографические указатели. Последовательность поиска документальных источников информации. Работа с книгой. Техника чтения.

6. Записи при чтении. Методы изучения документальных источников. Источники документации. Техника изучения документов. Классические методы. Контентный анализ. Фиксирование информации.

Продолжительность занятия- 4.0 /3 часов

**Тема 8. Способы оценки информации. Обеспечение безопасности и
защиты информации. Специальные аналитические технологии для
предупреждения и расследования противоправных посягательств на
безопасность**

Практическое занятие 8.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Источники информации. Взятие информации из документов. Принципы оценки и анализа информации.
2. Безопасность информационной работы.
3. Информационная безопасность организации (учреждения).
4. Элементы системы безопасности. Внутренняя безопасность. Локальная безопасность. Использование телефона. Организация встреч.
5. Защита информационных объектов. Виды угроз информационным объектам.
6. Методы и средства обеспечения информационной безопасности организации (фирмы).
7. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность.

Продолжительность занятия- 4.0 /3.0 часов

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: Место информационной безопасности в системе национальной безопасности. Современная концепция информационной безопасности. Цели и концептуальные основы защиты информации. <i>Самостоятельное изучение темы</i> (тематика определяется преподавателем)
2.	Особенности организации регионального управления информационной	Подготовка докладов по темам: Критерии, условия и принципы отнесения информации к защищаемой. Классификация конфиденциальной информации

	<p>безопасностью (требования к работе информационно-аналитических подразделений)</p>	<p>по видам тайны и степеням конфиденциальности. Понятие и структура угроз защищаемой информации. <i>Самостоятельное изучение темы</i> (тематика определяется преподавателем)</p>
3	<p>Основы построения систем информационно-аналитического обеспечения управления безопасностью в органах государственной власти и местного самоуправления региона</p>	<p>Подготовка докладов по темам: Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию. Причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемую информацию. Виды уязвимости информации и формы ее проявления. <i>Самостоятельное изучение темы</i> (тематика определяется преподавателем)</p>
4	<p>Инструментарий информационно-аналитической поддержки принятия решений в органах государственной власти и местного самоуправления региона</p>	<p>Подготовка докладов по темам:</p> <ol style="list-style-type: none"> 1. Международная система по противодействию легализации преступных доходов и финансированию терроризма, противодействие финансированию терроризма и экстремизма. 2. Формы и методы подготовки аналитической информации. 3. Информационные ресурсы в первичном (государственном) финансовом мониторинге. 4. Информационное взаимодействие и ресурсы в государственном финансовом мониторинге. 5. Основы контрольно-надзорной деятельности. 6. Международная гражданская служба. 7. Государственная гражданская служба в РФ. 8. Системы внутреннего контроля в субъектах финансового мониторинга; Финансовые расследования в международном (государственном) финансовом мониторинге. 9. Типологический анализ в первичном (государственном, международном) финансовом мониторинге. 10. Национальная система по противодействию легализации преступных доходов и финансированию терроризма. <p><i>Самостоятельное изучение темы</i> (тематика определяется преподавателем)</p> <p>Письменная работа Предложения руководителю для принятия решения в рамках ИАД по обеспечению безопасности функционирования объекта информатизации.</p>

5. Указания по проведению контрольных работ

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, сформированных 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 и оформлен с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению

Объем контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

5.4. Примерная тематика контрольных работ:

1. Информационно-аналитическая деятельность в системе государственных органов, неправительственных исследовательских, академических, коммерческих организаций.
2. Содержание и особенности информационно-аналитического обеспечения принятия управленческих решений.
3. Факты и события как единицы социальной информации, их соотношение. Процедура анализа фактов и событий, как элементов социальной информации.
4. Методологические особенности прикладного анализа политических ситуаций и процессов.
5. Информационные ресурсы прикладного социально-политического анализа.
6. Экспертное сопровождение политических решений (проблемы методики и организации).
7. Соотношение объекта и предмета исследования.
8. Процедура логического анализа ключевых понятий.
9. Особенности институционального анализа социально-политических процессов.

10. Бихевиористская парадигма прикладного социально-политического анализа.
11. Системный анализ социально-политических ситуаций и процессов.
12. Парадигма рационального выбора и её использование в прикладном социально-политическом анализе.
13. Ивент-анализ социально-политических процессов.
14. Контент-анализ и его роль в прикладном анализе социально-политических процессов.
15. Концептуальные и эмпирические основания оценки информационных источников. Критерии оценки информационных источников.
16. Опыт использования креативных технологий при выработке управленческих решений.
17. Технология «мозгового штурма» и её роль в выработке социально-политических управленческих решений.
18. Интернет — ресурсы как источник концептуально-аналитической информации по проблемам внутренней и внешней политики.
19. Дезинформация как средство политического манипулирования.
20. Признаки использования манипулятивных технологий в социально-политической коммуникации.
21. Содержание анализа при принятии социально-политического управленческого решения.
22. Структура информационных ресурсов принятия управленческого решения.
23. Критерии оценки достоверности информации.
24. Слухи как самотранслирующаяся коммуникация. Информационные и экспрессивные составляющие слуха.
25. Прогнозирование как разновидность информационно-аналитического обеспечения управленческих решений.
26. Типология методов прогнозирования. Субъективные и объективные, детерминированные и индетерменированные, линейные и нелинейные методы прогнозирования.
27. Экспертные методы прогнозирования. Разновидности экспертных процедур прогнозирования.
28. Оценка политических прогнозов средствами информационно-аналитического обеспечения принятия управленческих решений.
29. Понятие «обзорная информация». Информационный анализ и синтез, функции обзорной информации.
30. Разновидности информационно-аналитических документов.

6. Перечень основной и дополнительной учебной литературы

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:

3. 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.

4. 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.

5. 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.

6. С. И. Журин. Практика и теория использования детекторов лжи /- 2-е пзд., стереотип. - М.: Горячая линия-Телеком, 2011.

Белый В.М. Теория информационного менеджмента. Монография. Королев: «Канцлер», 2010.

7. А.А. Демидов, Ю.Н. Захаров. Информационно – аналитические системы принятия решений в органах государственной власти и местного самоуправления. Основы проектирования и внедрения. Учебное пособие. СПб: НИУ ИТМО, 2012.-100 с.

8. Д. В. Исаев. Аналитические информационные системы. Учебное пособие. ГУ ВШЭ.- М., 2008. - 60 с.

Л. А. Демидова. Принятие решений в условиях неопределенности /, В. В. Кираковский. А. Н. Пылькин. - М.: Горячая линия — ТВДИЖОМ, 2012.-288 с: ил.

9. Васильков А.В. Информационные системы и их безопасность. Учебное пособие.- М., ФОРУМ, 2010.

10. А.Ф. Чипига. Информационная безопасность автоматизированных систем. Учебное пособие.- Гелиос АРВ, 2010.

11. Гамза В.А., Ткачук И.Б. Безопасность банковской деятельности: учебник.- 2 –е изд., перераб. и доп. – М.: Маркет ДС, 2010.-408 с. (Университетская серия).

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

Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал
2. <http://informika.ru/> – образовательный портал
3. <http://www.academy.it.ru/> – академия АЙТИ
4. www.wikIsec.ru - Энциклопедия информационной безопасности - Публикации, статьи
5. www.biblioclub.ru - Универсальная библиотека онлайн
6. www.rucont.ru - ЭБС «Рукопт»
7. <http://www.minfin.ru> - Официальный сайт Министерства финансов Российской Федерации
8. <http://www.gov.ru/> - Официальный сервер органов государственной власти Российской Федерации
9. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности
10. <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, Multisim.*

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета
2. Информационно-справочные системы (Консультант+; Гарант).
3. Рабочая программа и методическое обеспечение по курсу «Основы конкурентной разведки».