МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ

Декан факультета
информационных технологий
/Д. Г. Демидов/

«28» апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информационная безопасность личности, общества и государства»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Профиль
«Безопасность открытых информационных систем»

Квалификация
Специалист по защите информации

Формы обучения
Очная

Москва, 2022 г.

Разработчик(и):
Разработчики:
Доцент кафедры «Информационная безопасность», к.т.н, доцент:


/ И.В. Калуцкий /

Доцент кафедры «Информационная безопасность», к.т.н., доцент, MBA


/ К.В. Пителинский /

Согласовано:
И.о. заведующего кафедрой «Информационная безопасность»,


А.Ю. Гневшев

Руководитель образовательной программы,


А.Ю. Гневшев

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Информационная безопасность личности, общества и государства» следует отнести:

- теоретическая и практическая подготовка специалистов в области обеспечения безопасности инноваций (в т. ч., в сфере информационных технологий и информационной безопасности).

К **основным задачам** освоения дисциплины «Информационная безопасность личности, общества и государства» следует отнести:

- овладение принципами проведения обеспечения информационной и экономической безопасности для личности, общества и государства.

Обучение по дисциплине **«Информационная безопасность личности, общества и государства»** направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК—1 – Способность оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИОПК-1.1 Знает основные понятия информатики, назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных; ИОПК-1.2. Умеет использовать программные и аппаратные средства персонального компьютера; ИОПК-1.3. Владеет навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.).
ПК-11 – Способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	ИПК-11.1. Знает: - основные понятия и методы в области управленческой деятельности; - порядок выработки и реализации управленческих решений; - содержание управленческой работы руководителя подразделения; - проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и систем; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем

	безопасности автоматизированных систем. ИПК-11.2. Умеет: - оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; - осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; - проводить мониторинг угроз безопасности компьютерных сетей; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; - администрировать подсистемы информационной безопасности автоматизированных систем. ИПК-11.3. Владеет: - навыками обоснования, выбора, реализации и контроля результатов управленческого решения; - навыками организации и обеспечения режима секретности; - навыками работы с технической документацией на ЭВМ и вычислительные системы.
ПК-14 – Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	ИПК-14.1. Знает: - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах принципы формирования политики информационной безопасности в автоматизированных системах. ИПК-14.2. Умеет: - эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; - разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем. ИПК-14.3. Владеет: - криптографической терминологией; - навыками анализа информационной инфраструктуры автоматизированной

	системы и ее безопасности; - навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.

2 Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность личности, общества и государства» относится к числу профессиональных учебных дисциплин обязательной части базового цикла (Б1.1) основной образовательной программы специалитета (Б1.48)

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ОП: «Управление информационной безопасностью», «Социально-психологические аспекты информационной безопасности».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных(е) единиц(ы) (144 часа) во втором семестре.

3.1 Виды учебной работы и трудоемкость
(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**72**	9	1-18
	В том числе:			
1.1	Лекции	36	9	1-18
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	36	9	2-18
2	**Самостоятельная работа**	**72**	9	2-18
2.1	Курсовой проект		9	2-18
3	**Промежуточная аттестация**			19-21
	Зачет/диф. зачет/экзамен	**Экзамен**	9	
	Итого:	**144**		

3.2 Тематический план изучения дисциплины
(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Раздел 1. Новые технологии и тенденции развития социоэкономических систем						
1.1	Представление информации и информационные технологии	3	1				2
1.2	Революции в образовании и экономика знаний.	3	1				2
1.3	Биоинформатика и социальное поведение.	3	1				2
1.4	Законодательство РФ в сфере информационной безопасности.	5	1		2		2
1.5	Знания как информационное оружие. Явные и неявные способы управления социоэкономическими системами.	3	1				2
1.6	Модели для выявления и анализа возможностей, рисков и угроз. Динамические контурные потоки в организации.	8	2		4		2
1.7	Управление знаниями, как новая функция управления. Структура и процесс управления знаниями. Основные компоненты УЗ.	3	1				2
1.8	Источники знаний в компании. Операционно-тактические и стратегические преимущества от применения УЗ в бизнесе.	3	1				2
1.9	Подготовка и планирование внедрения знаний. Внедрение системы управления знаниями и ее развитие.	5	1		2		2
1.10	Общение и обучение. Анализ хода реализации проекта.	6	2		2		2
2	Раздел 2. Основы противодействия конкурентной разведке и примышленному шпионажу	0					
2.1	Способы получения и оценки информации.	5	1		2		2
2.2	Методы поиска и вербовки информаторов.	3	1				2
2.3	Методы обеспечения результативного общения.	5	1		2		2
2.4	Методы целенаправленного воздействия на человека.	5	1		2		2
2.5	Обеспечение безопасности разведывательной работы.	5	1		2		2
2.6	Элементы системы безопасности. Внешняя безопасность. Внутренняя безопасность. Локальная безопасность.	7	1		2		4

2.7	Организация встреч. Проблемы безопасности бизнесмена.	8	2		2		4
2.8	Поиск и обезвреживание взрывных устройств.	4	2				2
3	Раздел 3. Защита от внутренних угроз информационной безопасности	0					
3.1	Введение в инсайдерские угрозы	3	1				2
3.2	Экосистема внутренних нарушителей: суть проблемы и классификация инсайдеров. Классификация инсайдерских угроз.	4	2				2
3.3	Проблема утечки конфиденциальной информации. Методы оценки эффективности в сфере защиты информации от утечек. Организационные меры защиты.	8	2		2		4
3.4	Кадровая безопасность. Нетрадиционные методы оценки персонала.	3	1				2
3.5	Управление изменениями в ИТ-инфраструктуре. Службы обмена мгновенными сообщениями и инсайдеры.	6	2		2		2
3.6	Новая парадигма внутренней ИТ-безопасности.	3	1				2
3.7	Выбор программного средства защиты. Выбор программно-аппаратного средства защиты.	7	1		2		4
3.8	Защита от утечек через сменные носители. Проблемы на пути внедрения защиты от утечек.	6			2		4
3.9	Проблемы корпоративного управления правами (ERM)	3	1				2
3.10	Трудности контентной фильтрации	10	2		4		4
3.11	Архивирование электронной корреспонденции. Сценарии использования централизованных архивов. Примеры внедрения	7	1		2		4
Итого		**144**	**36**		**36**		**72**

3.3 Содержание дисциплины

Раздел 1. Новые технологии и тенденции развития социоэкономических систем

Представление информации и информационные технологии. Революции в образовании и экономика знаний. Биоинформатика и социальное поведение. Законодательство РФ в сфере информационной безопасности. Знания как информационное оружие. Явные и неявные способы управления социоэкономическими системами. Модели для выявления и анализа возможностей, рисков и угроз. Динамические контурные потоки в организации. Управление знаниями, как новая функция управления. Структура и процесс управления знаниями. Основные компоненты УЗ. Источники знаний в компании. Операционно-тактические и стратегические преимущества от применения УЗ в бизнесе. Подготовка и планирование внедрения знаний. Внедрение системы управления знаниями и ее развитие. Общение и обучение. Анализ хода реализации проекта.

Раздел 2. Основы противодействия конкурентной разведке и примышленному шпионажу

Способы получения и оценки информации. Методы поиска и вербовки информаторов. Методы обеспечения результативного общения. Методы целенаправленного воздействия на человека. Обеспечение безопасности разведывательной работы. Элементы системы безопасности. Внешняя безопасность. Внутренняя безопасность. Локальная безопасность. Организация встреч. Проблемы безопасности бизнесмена. Поиск и обезвреживание взрывных устройств.

Раздел 3. Защита от внутренних угроз информационной безопасности

Введение в инсайдерские угрозы. Экосистема внутренних нарушителей: суть проблемы и классификация инсайдеров. Классификация инсайдерских угроз. Нормативная совместимость. Нормативные акты корпоративного управления: Федеральный закон «О персональных данных». Стандарт Банка России по ИБ Соглашение Basel II Кодекс корпоративного поведения ФСФР. Американский закон SOX Корпоративное управление. Проблема утечки конфиденциальной информации. Методы оценки эффективности в сфере защиты информации от утечек. Организационные меры защиты. Кадровая безопасность. Нетрадиционные методы оценки персонала. Управление изменениями в ИТ-инфраструктуре. Службы обмена мгновенными сообщениями и инсайдеры. Новая парадигма внутренней ИТ-безопасности. Выбор программного средства защиты. Выбор программно-аппаратного средства защиты. Защита от утечек через сменные носители. Проблемы на пути внедрения защиты от утечек. Юридические аспекты Проблемы корпоративного управления правами (ERM) Трудности контентной фильтрации Архивирование электронной корреспонденции. Нормативные акты в сфере архивирования почты Сценарии использования централизованных архивов. Примеры внедрения.

3.4 Тематика семинарских/практических и лабораторных занятий

Семинарские/практические занятия в учебном плане не запланированы.

3.4.2 Лабораторные занятия

Лабораторная работа 1 «Законодательство РФ в сфере информационной безопасности в интернете»

Лабораторная работа 2. «Модели для выявления и анализа возможностей, рисков и угроз. Динамические контурные потоки в организации.».

Лабораторная работа 3. «. Внедрение системы управления знаниями».

Лабораторная работа 4. «Анализ хода реализации проекта».

Лабораторная работа 5. «Способы получения и оценки информации».

Лабораторная работа 6. «Методы обеспечения результативного общения».

Лабораторная работа 7. «Методы целенаправленного воздействия на человека».

Лабораторная работа 8. «Обеспечение безопасности разведывательной работы».

Лабораторная работа 9. «Внешняя безопасность. Внутренняя безопасность. Локальная безопасность».

Лабораторная работа 10. «Проблемы безопасности бизнесмена и организация безопасных деловых встреч».

Лабораторная работа 11. «Методы оценки эффективности в сфере защиты информации от утечек».

Лабораторная работа 12. «Службы обмена мгновенными сообщениями».

Лабораторная работа 13. «Выбор программных и программно-аппаратных средств защиты».

Лабораторная работа 14. «Защита от утечек через сменные носители».

Лабораторная работа 15. «Контентная фильтрация».

Лабораторная работа 16. «Архивирование электронной корреспонденции».

3.5 Тематика курсовых проектов (курсовых работ)

Примерные темы:
1. Анализ методов блокировки контента на стороне провайдера.
2. Реализация системы блокировки контента по IP-адресу и протоколу.
3. Реализация системы блокировки контента по URL-адресу.
4. Реализация системы блокировки контента по DNS.
5. Реализация системы блокировки контента с помощью технологии DPI.
6. Методы противодействия социальной инженерии, рекомендации.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // Российская газета. № 237. 25.12.1993.
2. Гражданский кодекс Российской Федерации (Часть первая) от 30 ноября 1994 года N 51-ФЗ
3. Гражданский кодекс Российской Федерации (Часть вторая) от 26.01.1996 № 14-ФЗ // СЗ РФ. 1996. № 5. ст. 410.
4. Гражданский кодекс Российской Федерации часть 3 (ГК РФ ч.3) от 26 ноября 2001 года N 146-ФЗ
5. Гражданский кодекс Российской Федерации часть 4 (ГК РФ ч.4) от 18.12.2006 № 230-ФЗ
6. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СЗ РФ. 1996. № 25. ст. 2954.
7. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // СЗ РФ. 2001. № 52 (ч. I).ст. 4921.

8. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ // Российская газета. № 256., 31.12.2001.

9. Гражданский кодекс Российской Федерации (Часть четвертая) от 18.12.2006 № 230-ФЗ // СЗ РФ. 2006. № 52 (1 ч.).ст. 5496.

10. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» // СЗ РФ. 1997. № 41. стр. 8220-8235.

11. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» // СЗ РФ.1996. № 6. ст. 492.

12. Федеральный закон от 07.08.2001 № 119-ФЗ «Об аудиторской деятельности» // СЗ РФ. 2001. № 33 (часть I).ст. 3422.

13. Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной подписи» // СЗ РФ. 2002. № 2. ст. 127.

14. Федеральный закон "О лицензировании отдельных видов деятельности" от 04.05.2011 N 99-ФЗ

15. Федеральный закон "О техническом регулировании" от 27.12.2002 N 184-ФЗ

16. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // СЗ РФ. 2003. № 28. ст. 2895.

17. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // СЗ РФ. 2004. № 32. ст. 3283.

18. Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

19. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.).ст. 3448.

20. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (1 ч.).ст. 3451.

21. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"

22. Указ Президента РФ от 20.01.1996 N 71 "Вопросы Межведомственной комиссии по защите государственной тайны"

23. Указ Президента РФ от 16.08.2004 N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю"

24. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

25. Федеральный закон "О федеральной службе безопасности" от 03.04.1995 N 40-ФЗ

26. Федеральный закон от 31.05.1996 N 61-ФЗ «Об обороне»

27. Указ Президента РФ от 06.03.1997 N 188 "Об утверждении Перечня сведений конфиденциального характера"

28. Указ Президента РФ от 01.05.2022 N 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации"

29. Постановление Правительства РФ от 03.11.1994 N 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»

30. Постановление Правительства Российской Федерации от 3 февраля 2012 г. N 79 «О лицензировании деятельности по технической защите конфиденциальной информации»

31. Постановление Правительства Российской Федерации от 3 марта 2012 г. N 171 О лицензировании деятельности по разработке и производству средств защиты

конфиденциальной информации

32. Постановление Правительства РФ от 02.06.2008 N 418 "О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации"

33. Постановление Правительства РФ от 15.04.1995 N 333 (ред. от 03.02.2023) "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны"

34. Постановление Правительства РФ от 06.02.2010 N 63 (ред. от 10.07.2020) "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне"

35. Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) "О сертификации средств защиты информации"

36. Постановление Правительства РФ от 15.07.2022 N 1272 "Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)"

37. Приказ ФСБ РФ от 24.10.2022 № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств"

38. Приказ ФСБ России от 10.07.2014 N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности"

39. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

40. Приказ ФСТЭК России от 29 апреля 2021 г. N 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»

41. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

42. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

43. Приказ ФСТЭК России от 23 марта 2017 г. N 49 «О внесении изменений в состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. n 21, и в требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих

повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. n 31»

44. Приказ ФСТЭК России от 03.04.2018 N 55 (ред. от 19.09.2022) "Об утверждении Положения о системе сертификации средств защиты информации"

45. "Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021)

46. ГОСТ Р 53131-2008 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения».

47. ГОСТ Р ИСО/МЭК 27005-2010 Национальный стандарт российской федерации информационная технология методы и средства обеспечения безопасности менеджмент риска информационной безопасности

48. "ГОСТ Р ИСО/МЭК 27001-2021. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

49. ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности»

4.2 Основная литература

1. Криулин, А. А. Основы безопасности прикладных информационных технологий и систем : учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва : РТУ МИРЭА, 2020. — 136 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167606.
2. Нефедов, В. С. Основы обеспечения анонимности в сети Интернет : учебное пособие / В. С. Нефедов, А. А. Криулин, Г. Ю. Потерпеев. — Москва : РТУ МИРЭА, 2022. — 81 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/240041
3. Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания : учебное пособие / И. Д. Алекперов, В. В. Храмов, А. А. Горбачева, Д. С. Фомичев. — Ростов-на-Дону : ИУБиП, 2020. — 114 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/248747
4. Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для СПО / В. И. Петренко, И. В. Мандрица. 2-е изд., стер. - Санкт-Петербург: Лань, 2022. 108 с. – ISBN 978-5-8114-9038-7 — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/183744

4.3 Дополнительная литература

1. *Внуков, А. А.* Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст :

электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512269
2. Груздева, Л. М. Основы информационной безопасности : учебное пособие : в 2 частях / Л. М. Груздева. — Москва : РУТ (МИИТ), 2017 — Часть 1 — 2017. — 101 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/188704

4.4 Электронные образовательные ресурсы

1. Электронного образовательного ресурса по дисциплине «Информационная безопасность личности, общества и государства» нет.
2. Московский Политех подключен к ЭБС: Юрайт, АйПиАр и Лань
3. https://mospolytech.ru/obuchauschimsya/biblioteka/

4.5 Лицензионное и свободно распространяемое программное обеспечение

Для выполнения лабораторных работ и самостоятельной работы необходимо следующее программное обеспечение:

1. Microsoft Windows.
2. Веб-браузер, Chrome.

4.6 Современные профессиональные базы данных и информационные справочные системы

4. Справочная правовая система "КонсультантПлюс" *https://www.consultant.ru/*
5. Официальный сайт ФСТЭК России *https://fstec.ru/*
6. Образовательная платформа *«Юрайт»* *https://urait.ru/*

5 Материально-техническое обеспечение

И лекционные и лабораторные занятия могут проводится дистанционно в формате онлайн. Преподавателю для проведения занятий необходим ноутбук с возможностью использования сервиса корпоративной платформы Microsoft Teams или других платформ для проведения занятий, например, Zoom. У студентов должна быть возможность выхода в Интернет.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия

следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.2 Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов помогает получить дополнительные теоретические и практические знаниями по изучаемой дисциплине, развивает сознательное отношение к интеллектуальному труду.

В процессе самостоятельной работы, студенты дорабатывают конспекты лекций, готовятся к экзамену, изучают рекомендованную литературу, осуществляют подборку нормативно-правовых документов и проводят ознакомительный анализ с ними, готовятся к лабораторным работам, выполняют домашние задания;

Самостоятельная работа позволяет закрепить и углубить знания, полученные во время аудиторных занятий, а также изучить отдельные темы учебной программы.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Лекционные занятия дают общее представление по изучаемой теме, основной знания студент получает в процессе выполнения лабораторных работ и самостоятельной работы.

Практические занятия проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ. *Написание лабораторных работ* предполагает более детальное изучение нормативно-правовых документов, регламентирующих деятельность по защите информации, в рамках определённой тематики, а также обмен мнениями по поставленным *вопросам,* в процессе разбора проверенных работ.

Домашним заданием, по большей части, является подготовка к следующей лабораторной работе. Студентам предлагается выполнить подбор литературы, нормативно-правовых документов, по тематике лабораторной работы, и предварительное ознакомление с ними.

При проведении лабораторной работы преподаватель *выполняет, в основном,* функции ведущего - следит за регламентом времени, помогает уточнить формулировки, отвечает на вопросы студентов, проверяет выполненные работы. На следующем занятии, подводится итог проведенной работы, студентам сообщаются результаты, ведется обсуждение рассмотренных вопросов подводится итог занятию в целом.

По результатам выполнения всех видов учебной работы, предусмотренных учебным планом (подготовка конспектов лекций, успешное выполнение лабораторных работ, подготовка домашнего задания, присутствие и активная работа на занятиях) по данной дисциплине (модулю), преподаватель может рассмотреть возможность проставления положительной оценки на экзамене «Автоматом», при этом учитываются результаты

текущего контроля успеваемости в течение семестра. В случае, если студент длительно отсутствовал на занятиях, не выполнял задания он всё равно допускается до экзамена, но на экзамене, таким студентам, преподаватель может задавать любое количество вопросов по всем темам данной дисциплины (в рамках отведённого времени), дабы убедиться, что студент самостоятельно освоил дисциплину.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на зачёте в письменной (устной) форме.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- домашние задания и их защита;
- лабораторные работы,
- курсовой проект;
- экзамен.

7.2 Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю)

ОПК-1. Способность оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: основные понятия информатики, назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных	Обучающийся демонстрирует полное отсутствие знаний основных понятий информатики, назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных.	Обучающийся демонстрирует неполное соответствие знаний основных понятий информатики, назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает	Обучающийся демонстрирует частичное соответствие следующих знаний: основных понятий информатики, назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных, но допускаются	Обучающийся демонстрирует полное соответствие следующих знаний: основных понятий информатики, назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных,

		значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	незначительные ошибки, неточности, затруднения при аналитических операциях.	свободно оперирует приобре-тенными знаниями.
уметь: - Умеет использовать программные и аппаратные средства персонального компьютера;	Обучающийся не умеет или в недостаточной степени умеет использовать программные и аппаратные средства персонального компьютера.	Обучающийся демонстрирует неполное соответствие следующих умений: применять программные и аппаратные средства персонального компьютера. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: применять программные и аппаратные средства персонального компьютера. Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрируе т полное соответствие следующих умений: применять программные и аппаратные средства персонального компьютера. Свободно оперирует приобретенны ми умениями, применяет их в ситуациях повышенной сложности.
владеть: - навыками поиска информации в глобальной информационн ой сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационн ых материалов, СУБД и т.п.).	Обучающийся не владеет или в недостаточной степени владеет навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.).	Обучающийся владеет навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.)., допускаются значительные ошибки, проявляется недостаточность владения навыками.	Обучающийся частично владеет навыками поиска информации в глобальной информационно й сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационн ых материалов, СУБД и т.п.).. Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения.	Обучающийся в полном объеме владеет навыками поиска информации в глобальной информацион ной сети Интернет и работы с офисными приложениям и (текстовыми процессорами, электронными таблицами, средствами подготовки презентацион ных материалов, СУБД и т.п.)., свободно применяет полученные навыки в ситуациях

				повышенной сложности.
ПК-11 Способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности;				
Знает: - основные понятия и методы в области управленческой деятельности; - порядок выработки и реализации управленческих решений; - содержание управленческой работы руководителя подразделения; - проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и систем; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем.	Обучающийся не знает: - основные понятия и методы в области управленческой деятельности; - порядок выработки и реализации управленческих решений; - содержание управленческой работы руководителя подразделения, содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем	Обучающийся демонстрирует неполное знание: - основные понятия и методы в области управленческой деятельности; - порядок выработки и реализации управленческих решений; - содержание управленческой работы руководителя подразделения, содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное знание - основные понятия и методы в области управленческой деятельности; - порядок выработки и реализации управленческих решений; - содержание управленческой работы руководителя подразделения, содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует знание: - основные понятия и методы в области управленческой деятельности; - порядок выработки и реализации управленческих решений; - содержание управленческой работы руководителя подразделения, содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Свободно оперирует приобретёнными знаниями.

Умеет: - оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; - осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; - проводить мониторинг угроз безопасности компьютерных сетей; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; - администрировать подсистемы информационной безопасности автоматизированных систем.	Обучающийся не умеет: оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; - осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; - проводить мониторинг угроз безопасности компьютерных сетей; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; - администрировать подсистемы информационной безопасности автоматизированных систем.	Обучающийся демонстрирует неполное соответствие следующих умений: - оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; - осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; - проводить мониторинг угроз безопасности компьютерных сетей; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; - администрировать подсистемы информационной безопасности автоматизированных систем. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: - оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; - осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; - проводить мониторинг угроз безопасности компьютерных сетей; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; - администрировать подсистемы информационной безопасности автоматизированных систем. Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие умений: - оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; - осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; - проводить мониторинг угроз безопасности компьютерных сетей; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; - администрировать подсистемы информационной безопасности автоматизированных систем. Свободно оперирует приобретенными умениями,

				применяет их в ситуациях повышенной сложности.
Владеет: - навыками обоснования, выбора, реализации и контроля результатов управленческого решения; - навыками организации и обеспечения режима секретности; - навыками работы с технической документацией на ЭВМ и вычислительные системы.	Обучающийся не владеет: - навыками обоснования, выбора, реализации и контроля результатов управленческого решения; - навыками организации и обеспечения режима секретности; - навыками работы с технической документацией на ЭВМ и вычислительные системы.	Обучающийся владеет - навыками обоснования, выбора, реализации и контроля результатов управленческого решения; - навыками организации и обеспечения режима секретности; - навыками работы с технической документацией на ЭВМ и вычислительные системы, но допускаются значительные ошибки, проявляется недостаточность владения навыками.	Обучающийся частично владеет - навыками обоснования, выбора, реализации и контроля результатов управленческого решения; - навыками организации и обеспечения режима секретности; - навыками работы с технической документацией на ЭВМ и вычислительные системы. Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения.	Обучающийся в полном объеме владеет - навыками обоснования, выбора, реализации и контроля результатов управленческого решения; - навыками организации и обеспечения режима секретности; - навыками работы с технической документацией на ЭВМ и вычислительные системы.
ПК-14. Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации				

Знает: - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах принципы формирования политики информационной безопасности в автоматизированных системах.	Обучающийся не знает: - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах принципы формирования политики информационной безопасности в автоматизированных системах	Обучающийся демонстрирует неполное знание: - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах принципы формирования политики информационной безопасности в автоматизированных системах. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное знание - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах принципы формирования политики информационной безопасности в автоматизированных системах. Допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует знание: - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах принципы формирования политики информационной безопасности в автоматизированных системах. Свободно оперирует приобретёнными знаниями.
Умеет: - эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; - разрабатывать частные политики информационной безопасности информационн	Обучающийся не умеет: - эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; - разрабатывать частные политики информационной безопасности автоматизированных систем.	Обучающийся демонстрирует неполное соответствие следующих умений: - - эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; - разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: - - эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; - разрабатывать частные политики информационной безопасности информационной безопасности	Обучающийся демонстрирует полное соответствие умений: - - эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; - разрабатывать частные политики

ой безопасности автоматизированных систем.			автоматизированных систем. Умения освоены, но допускаются незначительные ошибки, неточности.	информационной безопасности информационной безопасности автоматизированных систем. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
Владеет: - криптографической терминологией; - навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; - навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем**.**	Обучающийся не владеет: - криптографической терминологией; - навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; - навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.	Обучающийся владеет - - криптографической терминологией; - навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; - навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем, но допускаются значительные ошибки, проявляется недостаточность владения навыками.	Обучающийся частично владеет - - криптографической терминологией; - навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; - навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем. Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения.	Обучающийся в полном объеме владеет - - криптографической терминологией; - навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; - навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.

Шкалы оценивания результатов промежуточной аттестации и их описание:
Форма промежуточной аттестации: дифференцированный зачёт

Промежуточная аттестация обучающихся, в форме экзамена, проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых

результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

7.3.1. Примерные вопросы по лабораторным работам

ТЕСТ-ВОПРОСЫ
по курсу: «Информационная безопасность личности, общества и государства»

Угрозы безопасности компьютерной информации

S: Под угрозой безопасности информации понимается:

-: Атака на информацию со стороны злоумышленника

+: Потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации

-: Несанкционированный доступ к информации, который может привести к нарушению целостности системы компьютерной безопасности

S: Все множество потенциальных угроз безопасности информации в КС может быть разделено на следующие классы:

+: Случайные угрозы

-: Потенциальные угрозы

+: Преднамеренные угрозы

-: Предсказуемые угрозы

S: Что понимается под возможным каналом утечки информации?

+: Способ, позволяющий нарушителю получить доступ к хранящейся или обрабатываемой информации

-: Техническое средство, с помощью которого нарушитель может получить доступ к хранящейся или обрабатываемой информации

-: Комплекс программных и/или аппаратных средств, позволяющих осуществлять передачу данных от источника информации к нарушителю

S: С помощью каких типов средств может происходить утечка информации по возможному каналу?

-: Данные

+: Человек

-: Компьютерная сеть

+: Программа

+: Аппаратура

S: При хранении, поддержании и предоставлении доступа к любому информационному ресурсу его владелец, либо уполномоченное им лицо, накладывает явно либо самоочевидно набор правил по работе с ней. Умышленное их нарушение классифицируется как ##### на информацию.

+: атака

S: Перечислите основные виды случайных угроз:

+: Стихийные бедствия и аварии

+: Сбои и отказы технических средств

+: Ошибки при разработке компьютерных систем

+: Алгоритмические и программные ошибки

+: Ошибки пользователей и обслуживающего персонала

-: Электромагнитные излучения и наводки

-: Вредительские программы

S: Перечислите основные виды преднамеренных угроз:

-: Алгоритмические и программные ошибки

+: Шпионаж и диверсии

+: Несанкционированный доступ (НСД) к информации

+: Электромагнитные излучения и наводки

+: Несанкционированная модификация структур

-: Стихийные бедствия и аварии

+: Вредительские программы

S: В зависимости от механизма действия вредительские программы делятся на:

+: Логические бомбы

-: Генераторы белого шума

-: Дизассемблеры

+: Черви

+: Троянские кони

+: Компьютерные вирусы

-: Декомпиляторы

S: К наиболее распространенным методам взлома можно отнести следующие:

-: Подбор пароля с помощью генераторов случайных чисел

+: Доступ к информации через терминалы защищенной информационной системы

+: Получение пароля на основе ошибок администратора и пользователей

+: Получение пароля на основе ошибок в реализации системы

-: Деактивация функций операционной системы (ОС)

+: Социальная психология

+: Комплексный поиск возможных методов доступа

S: Установите соответствие между конкретным методом взлома и классом, к которому он относится.

L1: Социальная психология

L2: Получение пароля на основе ошибок в реализации системы

L3: Получение пароля на основе ошибок администратора и пользователей

L4: Доступ к информации через терминалы защищенной информационной системы

R1: Звонок клиенту от лица администратора

R2: Получение пароля из самой системы

R3: Перебор паролей по словарю

R4: Вход через официальный log-in запрос системы

7.3.2 Примерный список вопросов для экзамена

1. Представление информации и информационные технологии. Революции в образовании и экономика знаний.
2. Новые технологии и тенденции развития техносферы. Биоинформатика и социальное поведение. Биокибернетика. Нанотехнологии.
3. Приоритеты управления и полный вектор управления. Знания как информационное оружие. Законодательство РФ в сфере информационной безопасности. Явные и неявные способы управления социоэкономическими системами.
4. Модели для выявления и анализа возможностей, рисков и угроз. Прогнозное планирование: определение рисков и поиск возможностей.
5. Методы прогнозирования рисков. Динамические контурные потоки в организации.
6. Управление знаниями. Основные понятия и определения. Управление знаниями, как новая функция управления. Структура системы знаний. Основные компоненты УЗ.
7. Операционно-тактические и стратегические преимущества от применения УЗ в бизнесе. Перспективы применения УЗ в бизнесе. Анализ хода реализации проекта.
8. Нейронные сети, нечеткие множества и интеллектуальные информационные системы
9. Статические и динамические экспертные системы. Приобретение знаний. Извлечение знаний из данных. Источники знаний в компании. Поиск информации в Интернет
10. Нейронные сети. Принципы работы и сфера применения
11. Техносфера и человеко-машинное взаимодействие История ВТ и мультимедиа.
12. Техносфера и человеко-машинное взаимодействие Робототехника и мехатроника.
13. Конкурентная разведка и примышленный шпионаж. Сходство и различие
14. Способы получения и оценки информации Краткая характеристика источников информации. Взятие информации из средств связи. Взятие информации через отслеживание. Использование слухов.
15. Принципы оценки и анализа информации. Достоверность и надежность материалов. Искажение информации и дезинформация. Техника интерпретации данных
16. Выявление и разработка кандидата. Установление и Углубление контакта. Составление досье. Тактика оценки кандидата. Проведение вербовки.
17. Обхождение с завербованным и направление его деятельности. Способы удержания. Способы проверки. Способы связи. Завершение контакта
18. Теория и практика результативного общения. Общие рекомендации по организации. Психофизиологические аспекты. Составные элементы общения. Точность восприятия партнера по общению.
19. Методы обеспечения результативного общения. Методы целенаправленного воздействия на человека. Обеспечение безопасности разведывательной работы
20. Элементы системы безопасности. Обеспечение тайны посланий: криптография. Шифрование. Дешифровка. Стеганография

21. Проблемы безопасности бизнесмена О личном оружии. Требования к телохранителю. Животные-защитники.
22. Проблемы безопасности бизнесмена Общие меры защиты от покушений. Защита автомобиля и квартиры Поведение при похищении. Защита от технических средств. создание своей службы безопасности.
23. Защита от внутренних угроз информационной безопасности. Классификация инсайдеров. Классификация инсайдерских угроз Угроза утечки конфиденциальной информации.
24. Обход средств защиты от утечки конфиденциальной информации. Кража конфиденциальной информации по неосторожности. Нарушение авторских прав на информацию. Мошенничество.
25. Нецелевое использование информационных ресурсов компании. Саботаж ИТ-инфраструктуры. Проблема утечки конфиденциальной информации Портрет респондентов.
26. Внутренние угрозы ИБ. Утечка конфиденциальной информации. Нормативное регулирование. Средства защиты
27. Методы оценки эффективности в сфере защиты информации от утечек
28. Организационные меры защиты Психологические меры. Права локальных пользователей. Стандартизация ПО. Работа с кадрами. Внутрикорпоративная нормативная база.
29. Хранение физических носителей. Система мониторинга работы с конфиденциальной информацией. Аутсорсинг хранения информации
30. Кадровая безопасность Нетрадиционные методы оценки персонала Увольнение работников: Увольнение и трудоустройство уволенных
31. Управление изменениями в ИТ-инфраструктуре Служба ИБ в структуре современной организации.
32. Парадигма внутренней ИТ-безопасности периметральная и канальная защита
33. Средства внутреннего контроля. Системы сильной аутентификации. Предотвращение нецелевого использования ИТ-ресурсов
34. Выбор программного средства защиты от утечек. Службы обмена мгновенными сообщениями и инсайдеры.
35. Выбор аппаратного средства защиты от утечек. Защита от утечек через сменные носители
36. Проблемы на пути внедрения защиты от утечек. Внешние угрозы. Внутренние угрозы.
37. Юридические аспекты. Проблемы корпоративного управления правами (ERM)
38. Решение проблемы резервного копирования. Стимулы к использованию центральных архивов. Требования к системам архивирования. Архивирование интернет-данных.
39. Сценарии использования централизованных архивов Расследование инцидентов ИБ
40. Архивирование электронной корреспонденции. Нормативные акты в сфере архивирования почты Трудности контентной фильтрации