Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Институт общественных наук
(наименование института (факультета))
Прикладных информационных технологий
(наименование кафедры)

Утверждена

решением кафедры Прикладных информационных технологий ИОН РАНХиГС

Протокол № 3

от «25» мая 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.06. Защита информации в организационных структурах
(индекс и наименование дисциплины, в соответствии с учебным планом)

38.04.02 Менеджмент
(направление подготовки)

"Digital design в менеджменте (информационно-аналитический менеджмент)"
программа магистратуры

Магистр
квалификация

очная
форма(ы) обучения

Год набора - 2021

Москва, 2020 г.

Автор–составитель:
Канд. эконом. наук, доцент кафедры
прикладных информационных технологий Федосеев А.И.
(ученое звание, ученая степень, должность) *(наименование кафедры)*
(Ф.И.О.)

Заведующий кафедрой прикладных ИТ к.т.н. _ Голосов П.Е.
(наименование кафедры) *(ученая степень и(или) ученое звание)* *(Ф.И.О.)*

СОДЕРЖАНИЕ

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

1.1. Дисциплина Б1.В.06 «Защита информации в организационных структурах» обеспечивает овладение следующими компетенциями с учетом этапа:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-1	способен управлять организациями, подразделениями, группами (командами) сотрудников, проектами и сетями	ПК-1.3	Владеть навыками управления проектами и сетями

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ *(при наличии профстандарта)*/ профессиональные действия	Код этапа освоения компетенции	Планируемые результаты обучения
Управление группой менеджеров продуктов - С/05.6	ПК-1.2	на уровне знаний: знать особенности управления организациями, подразделениями и группами сотрудников
		на уровне умений: уметь сравнивать различные стратегии и программы управления организациями, подразделениями и группами (командами) сотрудников
		на уровне навыков: владеть навыками управления проектами и сетями

2. Объем и место дисциплины в структуре ОП ВО

2.1. Объем дисциплины

Общая трудоемкость дисциплины Б1.В.06 «Защита информации в организационных структурах» составляет 2 зачётные единицы. Дисциплина реализуется с применением дистанционных образовательных технологий (далее - ДОТ).

Количество академических часов, выделенных на контактную работу с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся:

очная форма обучения:

− лекции (контактные аудиторные часы) – 8 ч.;

− лабораторные занятия (контактная работа, аудиторно) –16 ч;

− контролируемая самостоятельная работа (с применением ДОТ) –20 ч.;

− самостоятельная работа (с применением ДОТ) –28 ч.;

- форма промежуточной аттестации в соответствии с учебным планом – зачет.

2.2. Место дисциплины в структуре ОП ВО.

В соответствии с учебным планом дисциплина Б1.В.06 «Защита информации в организационных структурах» входит в состав дисциплин части, формируемой участниками образовательных отношений и изучается в __2__ семестре 1 курса в соответствии с учебным планом одновременно с такими дисциплинами, как Б1.В.03 «Поиск и обработка информации в неструктурированных массивах данных (Data Mining)», Б1.В.ДВ.01.01 «Статистические методы в аналитической работе», после дисциплин Б1.Б.01 «Современный менеджмент», Б1.В.01 «Современный маркетинг», Б1.В.02 «Основы разработки интернет-ресурсов», Б1.В.04 «Теория систем и системный анализ», Б1.О.05 «Методы исследований в менеджменте», Б1.О.06 «Современные коммуникации в менеджменте»

2.3. Регламент распределения видов работ по дисциплине с ДОТ

Данная дисциплина реализуется с применением дистанционных образовательных технологий (ДОТ). Распределение видов учебной работы, форматов текущего контроля представлены в таблице:

Вид учебной работы	Формат проведения

Лекционные занятия	Контактные аудиторные часы
Лабораторные занятия	Контактные аудиторные часы
контролируемая самостоятельная работа	С применением ДОТ
Самостоятельная работа	С применением ДОТ
Промежуточная аттестация	Контактная аудиторная работа
Формы текущего контроля	**Формат проведения**
Тестирование	Частично с применением ДОТ
Эссе	Частично с применением ДОТ
Ответ на практическом занятии, участие в дискуссии	Контактная аудиторная работа

Доступ к системе дистанционных образовательных осуществляется каждым обучающимся самостоятельно с любого устройства на портале: https://lms.ranepa.ru. Пароль и логин к личному кабинету / профилю предоставляется студенту в деканате.
Преподаватель оценивает выполненные обучающимся работы не позднее 10 рабочих дней после окончания срока выполнения.

3. Содержание и структура дисциплины

3.1. Очная форма обучения

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости[4], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР/ ЭО, ДОТ	
			Л	ЛР	ПЗ	КСР/ ЭО, ДОТ		
Очная форма обучения								
Тема 1	Введение. Безопасность функционирования современной организации и технологий.	8	2			3	4	О, Д, ЛР, Э, Т
Тема 2	Современная доктрина информационной безопасности Российской Федерации.	10	2			3	4	О, Д, ЛР, Э, Т
Тема 3	Международные стандарты информационного обмена. Модели безопасности и их применение.	12		4		3	4	О, Д, ЛР, Э, Т
Тема 4	Сущность и задачи обеспечения информационной безопасности.	14	2	4		3	4	О, Д, ЛР, Э, Т
Тема 5	Отечественные программно-аппаратные средства криптографической защиты компьютерных систем.	12		4		3	4	О, Д, ЛР, Э, Т
Тема 6	Состав, структура и назначение Удостоверяющих центров в системах защиты и аутентификации электронных документов в интернет.	16	2	4		5	4	О, Д, ЛР, Э, Т
Промежуточная аттестация							4	зачет
Всего:		72	8	16		20	28	

Примечание: 4 – формы текущего контроля успеваемости: опрос (О), лабораторная работа (ЛР), Д (дискуссия), Э (эссе), Т (тестирование)

3.2. Содержание дисциплины

Тема 1. Введение. Безопасность функционирования современной организации и технологий.

Введение. Предмет и задачи дисциплины. Значение и место дисциплины в подготовке специалистов в области прикладных аспектов информатики и информационных технологий по защите информации от несанкционированных воздействий и обеспечения достоверности и целостности при ее обработке в информационно-телекоммуникационных системах. Научная и учебная взаимосвязь дисциплины с другими дисциплинами, изучаемыми в высшем учебном заведении.

Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения практических и семинарских занятий. Состав и методика самостоятельной работы студентов по изучению дисциплины. Форма проверки знаний. Анализ нормативных источников, научной и учебной литературы. Знания и умения студентов, которые должны быть получены в результате изучения дисциплины.

Актуальность проблемы обеспечения информационной безопасности в торгово-экономических структурах, потенциально возможные несанкционированные воздействия на информационную инфраструктуру торгово-экономической деятельности, информационный криминал. Статистические показатели состояния информационной безопасности информационной инфраструктуры торгово-экономической деятельности, динамика ее развития.

Составляющие воздействий на информационную инфраструктуру государства: информационная война, информационный терроризм, информационный криминал. Понятие конкурентной разведки.

Тема 2. Современная доктрина информационной безопасности Российской Федерации.

Понятие и назначение Доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере. Значение информационной безопасности и ее место в системе национальной безопасности. Значение информационной безопасности для субъектов информационных отношений. Связь между информационной безопасностью и безопасностью информации.

Международные стандарты информационного обмена, правовые основы защиты государственной, коммерческой, служебной, процессуальной, профессиональной тайны и информации персонального характера. Федеральные Законы Российской Федерации по обеспечению информационной безопасности в информационных технологиях, Доктрина Информационной безопасности Российской Федерации, Концепция Национальной Безопасности Российской Федерации, нормативные и руководящие документы, Постановления Правительства Российской Федерации по проблемам обеспечения информационной безопасности, Руководящие документы и инструкции Федеральной службы по техническому и экспортному контролю (ФСТЭК), Приказы и распоряжения ФСБ РФ, Ведомственные приказы и распоряжения.

Тема 3. Международные стандарты информационного обмена. Модели безопасности и их применение.

Безопасность в сетях Internet и Intranet. Технология безопасности: межсетевые экраны (Межсетевые экраны прикладного уровня, межсетевые экраны с пакетной фильтрацией, гибридные межсетевые экраны). Разработка конфигурации межсетевого экрана: Архитектура 1 – системы за пределами; архитектура 2 – один межсетевой экран;

архитектура 3 – двойные межсетевые экраны. Безопасность виртуальных частных сетей (VPN).

Модели безопасности: модели разграничения доступа; модели разграничения доступа, построенные по принципу предоставления прав; модели дискретного доступа; модели мандатного доступа; модель Белла и Лападула; специализированные модели; вероятностные модели; информационные модели; модели контроля целостности; Модель Биба; модель Кларка-Вилсона. Модели анализа безопасности программного обеспечения.

Тема 4. Сущность и задачи обеспечения информационной безопасности.

Сущность информационной безопасности. Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Агрегация информационных ресурсов с точки зрения информационной безопасности. Классификация угроз информационной безопасности. Информационная безопасность компьютерных систем. Основные понятия и определения. Безопасность автоматизированных систем обработки информации. Доступ к информации (санкционированный, несанкционированный), разграничение доступа, конфиденциальность данных, угрозы безопасности, защита информации, политика безопасности

Основные виды угроз безопасности компьютерным системам: нарушения конфиденциальности информации, нарушения целостности информации, нарушения работоспособности системы. Каналы несанкционированного доступа. Способы несанкционированного доступа: перехват паролей, «маскарад», незаконное использование привилегий.

Тема 5. Отечественные программно-аппаратные средства криптографической защиты компьютерных систем.

«Врожденные слабости» наиболее распространенных служб Internet. Основные компоненты межсетевых экранов: фильтрующие маршрутизаторы, шлюзы сетевого уровня, шлюзы прикладного уровня. Аутентификация пользователей как основной компонент межсетевых экранов. Схема защиты компьютерных сетевых технологий на основе межсетевых экранов: фильтрующий маршрутизатор, межсетевой экран на основе двупортового шлюза, межсетевой экран на основе экранированного шлюза, экранированная подсеть, межсетевые экраны для организации виртуальных корпоративных сетей. Программные методы защиты сетевых технологий в Internet структурах.

Тема 6. Состав, структура и назначение Удостоверяющих центров в системах защиты и аутентификации электронных документов в интернет.

Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования, Разновидности задач защиты от копирования. Подходы к задаче защиты от копирования. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования. Привязка к внешним (добавляемым) элементам ПЭВМ. Привязка к портовым ключам. Использование дополнительных плат расширения. Методы «водяных знаков» и методы «отпечатков пальцев».

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

С применением ДОТ проводятся тестирования. Для успешного освоения курса учащемуся рекомендуется ознакомиться с литературой, размещенной в разделе 6.

4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации.

4.1.1. В ходе реализации дисциплины «Защита информации в организационных структурах» используются следующие методы текущего контроля успеваемости обучающихся:

− при проведении занятий лекционного типа (аудиторно): опрос, дискуссия;

− при проведении занятий практического (лабораторного) типа (аудиторно): опрос, дискуссия (устные ответы на вопросы преподавателя по теме занятия, групповое обсуждение вопросов); преподаватель, реализующий дисциплину, определяет самостоятельно планы занятий;

− при контроле результатов самостоятельной работы студентов (с использованием ДОТ): эссе, тестирование.

№	Тема и / или раздел	Методы текущего контроля успеваемости в аудитории	Методы текущего контроля успеваемости с применением ДОТ
1.	Тема 1. Введение. Безопасность функционирования современной организации и технологий.	Опрос, лабораторная работа, дискуссия	Эссе, тестирование
2.	Тема 2. Современная доктрина информационной безопасности Российской Федерации.	Опрос, лабораторная работа, дискуссия	Эссе, тестирование
3.	Тема 3. Международные стандарты информационного обмена. Модели безопасности и их применение.	Опрос, лабораторная работа, дискуссия	Эссе, тестирование
4	Тема 4. Сущность и задачи обеспечения информационной безопасности.	Опрос, лабораторная работа, дискуссия	Эссе, тестирование
5	Тема 5. Отечественные программно-аппаратные средства криптографической защиты компьютерных систем.	Опрос, лабораторная работа, дискуссия	Эссе, тестирование
6	Тема 6. Состав, структура и назначение Удостоверяющих центров в системах защиты и аутентификации электронных документов в интернет.	Опрос, лабораторная работа, дискуссия	Эссе, тестирование

4.2. Материалы текущего контроля успеваемости обучающихся

4.2.1. Типовые оценочные материалы

4.2.1.1. Примерные типовые тестовые здания

1. **Проекты, формы** и **модули интернет-приложений** сохраняются с расширениями:

- □ *.vba, *.fex, *.mex;
- □ *.vbp, *.frm, *.bas;
- □ *.exe, *.com, *.bat;
- □ *.htm, *.html

2. **Макросы** и **процедуры** проекта в приложениях сохраняются в разделе проводника:

- □ Macros;
- □ Project;
- □ Module;

3. Свойство **ControlSourse** элемента управления хранит в себе:

- □ Значение присоединенных к элементу данных;
- □ Диапазон присоединенных к элементу данных;
- □ Количество присоединенных к элементу данных;

4. Свойство **BoundValue** хранит в себе:

- □ Количество элементов, находящихся в данный момент в фокусе;
- □ Значение элемента, находящегося в данный момент в фокусе;
- □ Количество связанных между собой элементов;

5. Оператор **Range** задает:

- □ Допустимый в процедуре формат данных;
- □ Допустимый диапазон значений данных;
- □ Обращение к конкретной ячейке или диапазону ячеек;

6. Для того чтобы создать **присоединенный элемент управления** нужно:

- □ Вызвать панель инструментов *Формы* для выбора элемента;
- □ Вызвать панель инструментов *Visual Basic* для выбора элемента;
- □ Вызвать панель инструментов *Элементы управления* для выбора элемента;

7. Для того чтобы войти в **редактор JavaScript** нужно:

- □ Подать команду *Сервис* \ *Макрос* \ *Редактор Visual Basic*;
- □ Вызвать панель инструментов *Visual Basic*;
- □ Нажать клавиши Alt + F11;

8. Вновь записываемый **макрос** может быть доступен:

- □ Только для шаблона Normal.dot;
- □ Только для текущего документа;
- □ Для шаблона Normal.dot или для текущего документа;

9. **Пользовательскую панель инструментов** в можно создать с помощью:

- □ Команды *Сервис* \ *Настройка*, вкладка *Панели инструментов*;
- □ Команды *Вставка* \ *Объект*, параметр *Пакет*;
- □ Команды *Вид* \ *Панели инструментов* \ *Настройка*;
- □ Команды *Вид* \ *Линейка*;

10. **Кнопку для макроса** можно создать с помощью:

- □ Команды *Сервис* \ *Настройка*, вкладка *Команды*;
- □ Команды *Правка* \ *Специальная вставка*;
- □ Команды *Формат* \ *Тема*;

11. Каждый раз при записи **макроса** в проводник проекта добавляется:

- □ Модуль NewMacrosN() в раздел Normal;
- □ Модуль NewMacrosN() в раздел Project;
- □ Процедура Sub <Имя_Макроса>N()...End Sub в модуль NewMacros;

12. **Библиотека динамической компоновки** это:

- □ Файл с расширением *.sys, хранящий все пользовательские настройки;

- □ Файл с расширением *.ini, инициализирующий все макросы, записанные пользователем;
- □ Файл с расширением *.dll, содержащий функции, доступные для коррекции пользователем;

13. Оператор **Alias** указывает:

- □ наличие ошибки в функции из динамической библиотеки;
- □ название (имя) функции, используемое внутри файла *.dll;
- □ наличие вируса в макросе, использующем функцию из динамической библиотеки;

4.2.1.1. Примеры текстов, размещенных в СДО для прочтения и обсуждения в рамках дискуссии на практическом занятии (аудиторно)

№	Тема или раздел	Текст, размещенный в СДО	Методы текущего контроля успеваемости с применением ДОТ
1.	Тема 1. Введение. Безопасность функционирования современной организации и технологий.	Запечников С.В., Казарин О.В., Тарасов А.А КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ. М: Юрайт, 2016.	Ответы на открытые вопросы
2.	Тема 2. Современная доктрина информационной безопасности Российской Федерации.	Васильева И.Н. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ. - М: Юрайт, http://www.biblio-online.ru/, 2016.	Ответы на открытые вопросы

4.3. Оценочные средства для промежуточной аттестации

4.3.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Показатели и критерии оценивания компетенций с учетом этапа их формирования

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-1	способен управлять организациями, подразделениями, группами (командами) сотрудников, проектами и сетями	ПК-1.3	Владеть навыками управления проектами и сетями

Этап освоения компетенции / Дескриптор	**Показатель оценивания / Индикатор Что делает обучающийся (какие действия способен выполнить), подтверждая этап освоения компетенции**	**Критерий оценивания Как (с каким качеством) выполняется действие. Соответствует оценке «отлично» в шкале оценивания в РПД.**
ПК-1.3	Обучающийся выполняет функции корпоративного управления и регулирования.	Обучающийся отлично решает сложные управленческие задачи, в том числе в условиях турбулентности и неопределенности внешней среды.

4.3.2 Типовые оценочные средства

Материалы текущего контроля успеваемости

Типовые вопросы опроса

1. Основные виды угроз безопасности компьютерных систем.
2. Угрозы нарушения целостности информации, угрозы нарушения работоспособности АСОИ и отказы в работе.
3. Структурные составляющие гипотетической модели нарушителя.
4. Преднамеренные потенциальные угрозы. Классификация каналов несанкционированного доступа.
5. Наиболее распространенные способы несанкционированного доступа в компьютерных технологиях.
6. Перехват паролей, маскарад, незаконное использование привилегий, пассивное вторжение в АСОИ, активное вторжение.
7. Основные подходы для парирования и нейтрализации угроз информационной безопасности: фрагментарный подход и комплексный подход.

Примерные темы эссе/дискуссии:

1. Политика безопасности.

2. Виды политики безопасности: избирательная политика безопасности, полномочная политика безопасности.
3. Этапы построения системы защиты автоматизированных информационных систем.
4. Составляющие отдельных этапов.
5. Основные задачи методов защиты информации в автоматизированных информационных системах.
6. Принципы системы защиты информации в АСОИ.

***Любая проблема, связанная с защитой информации в организационных структурах и предложения по ее решению (по выбору обучающегося).**

Примерный перечень вопросов к зачету

1. Понятие «Информационная безопасность». Основные методологические и нормативно-правовые документы по информационной безопасности.

2. Основные понятия по защите компьютерных данных. Доступ к информации, санкционированный доступ, несанкционированный доступ, конфиденциальность данных, субъект и объект информационных технологий, доступность компонента или ресурса системы, угроза безопасности автоматизированной информационной системе, ущерб безопасности, уязвимость АСОИ, атака на компьютерную систему, политика безопасности.

3. Основные виды угроз безопасности компьютерных систем, Угрозы нарушения целостности информации, угрозы нарушения работоспособности АСОИ и отказы в работе.

4. Структурные составляющие гипотетической модели нарушителя, Преднамеренные потенциальные угрозы. Классификация каналов несанкционированного доступа.

5. Наиболее распространенные способы несанкционированного доступа в компьютерных технологиях. Перехват паролей, маскарад, незаконное использование привилегий, пассивное вторжение в АСОИ, активное вторжение.

6. Основные подходы для парирования и нейтрализации угроз информационной безопасности: фрагментарный подход и комплексный подход.

7. Политика безопасности. Виды политики безопасности: избирательная политика безопасности, полномочная политика безопасности.

8. Этапы построения системы защиты автоматизированных информационных систем. Составляющие отдельных этапов.

9. Основные задачи методов защиты информации в автоматизированных информационных системах. Принципы системы защиты информации в АСОИ.

10. Принципы криптографической защиты информации. Криптология, криптография, стеганография, криптоанализ. Три класса криптографических систем.

11. Традиционные симметричные криптографические системы. Ключ шифрования данных, шифры криптографической защиты данных: шифры перестановок, шифры замены, шифры гаммирования, шифры, основанные на аналитических преобразованиях шифруемых данных.

12. Шифрующие таблицы без ключевого слова.

13. Табличное шифрование методов перестановки по ключевому слову или фразе, задающими перестановку.

14. Табличное шифрование методом двойной перестановки.

15. Шифр Цезаря.

16. Метод аффинной системы подстановок Цезаря.

17. Система шифрования Цезаря с ключевым словом.

18. Одноалфавитные монограммные таблицы Трисимуса.

19. Шифры сложной замены. Шифр Гронсфельда.

20. Система шифрования Вернама.
21. Шифрование методом гаммирования.
22. Современные симметричные криптосистемы.
23. Стандарт шифрования DES.
24. Алгоритм шифрования IDEA.
25. Отечественный стандарт шифрования данных ГОСТ 28147-89.
26. Концепция криптографической системы с открытым ключом. Система асимметричной криптографической системы.
27. Однонаправленные Хэш-функции.
28. Криптографическая система шифрования данных RSA.
29. Процедура шифрования и расширения данных в криптографической системе RSA.
30. Безопасность и быстродействие криптографической системы RSA.
31. Схема шифрования Полига-Хелмана.
32. Схема шифрования Эль Гамаля.
33. Комбинированный метод шифрования данных.
34. Электронная цифровая подпись. Правовые основы электронной цифровой подписи. Федеральный закон РФ «Об электронной подписи.
35. Проблема аутентификации данных и электронная цифровая подпись.
36. Однонаправленные Хэш-функции. Алгоритмы электронной цифровой подписи.
37. Алгоритм ЭЦП RSA.
38. Алгоритм ЭЦП Эль Гамаля.
39. Алгоритм ЭПЦ DSA.
40. Отечественный стандарт электронной цифровой подписи ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001.
41. Идентификация и проверка подлинности электронных документов и пользователей компьютерных технологий.
42. Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверки подлинности пользователей.
43. Процедура «рукопожатия».
44. Протоколы аутентификации с нулевой передачей знаний.
45. Параллельная идентификация с нулевой передачей знаний.
46. Система идентификации Гиллоу-Куискуотера.
47. Управление криптографическими ключами. Генерация и хранение ключей.
48. Иерархия ключей шифрования данных в корпоративных компьютерных системах.
49. Распределение ключей в корпоративных компьютерных системах. Использование одного или нескольких центров распределении ключей. Прямой обмен сеансовыми ключами между санкционированными пользователями.
50. Механизм запроса – ответа в сетевых технологиях, механизм отметки времени.
51. Распределение ключей с участием Центра распределении ключей.
52. Протокол для симметричных криптосистем с использованием отметки времени.
53. Протокол для асимметричных криптосистем с использованием сертификатов открытых ключей.
54. Алгоритм открытого распределения ключей Диффи-Хелмана.
55. Протокол SKIP управления криптоключами.
56. Аутентификация пользователей как основной компонент межсетевых экранов.

57. Схема защиты компьютерных сетевых технологий на основе межсетевых экранов: фильтрующий маршрутизатор, межсетевой экран на основе двупортового шлюза, межсетевой экран на основе экранированного шлюза, экранированная подсеть, межсетевые экраны для организации виртуальных корпоративных сетей.

58. Программные методы защиты сетевых технологий в Internet структурах.

59. Защита данных в электронных платежных системах.

60. Принципы функционирования электронных платежных систем.

61. Электронные пластиковые карты. Пассивные и активные пластиковые карты. Основные типы активных пластиковых карт: карты-счетчики, карты с памятью, карты с микропроцессором, карты с контактным считыванием, карты с индукционным считванием.

62. Персональный идентификационный номер (PIN). Обеспечение безопасности электронно-платежной системы POS (Point-of-Sale), схема функционирования POS.

63. Обеспечение безопасности банкоматов в электронных платежных системах, схема обмена сообщениями между банкоматом и хост-ЭВМ банка рои идентификации и платеже, схема прохождения данных с PIN клиента между банкоматом, банком-эквайером и банком-эмитентом.

64. Универсальная платежная система UEPS (Universal Electronic Payment System), состав и архитектура платежной системы, распределение ключей и паролей, цикл платежной транзакции.

65. Торговые терминалы, формирование сессионных ключей, эмиссия карточек, разграничение ответственности между банками-участниками общей платежной системы, двойное шифрование записи о транзакции на ключах банка-эквайера и банка-эмитента.

66. Обеспечение безопасности электронных платежей через сеть Internet.

67. Авторизация и шифрование финансовой информации в сети Internet.

68. Протоколы шифрования SSL (Secure Socket Layer) и SET (Secure Electronic Transactions), использование сертификатов.

69. Отечественные программно-аппаратные средства криптографической защиты компьютерных систем.

70. Средства и системы управления контролем доступа в компьютерных технологиях.

71. Основные подходы к защите данных от несанкционированного доступа. Шифрование. Контроль доступа. Разграничения доступа к файлам.

72. Защита программного продукта от несанкционированного копирования.

73. Несанкционированное копирование программ как тип НСД.

74. Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования.

75. Разновидности задач защиты от копирования. Подходы к задаче защиты от копирования.

76. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования.

77. Привязка к внешним (добавляемым) элементам ПЭВМ. Привязка к портовым ключам. Использование дополнительных плат расширения.

78. Методы «водяных знаков» и методы «отпечатков пальцев».

79. Защита программного продукта от изучения.

80. Изучение и обратное проектирование программного обеспечения: понятие изучения и обратного проектирования программного обеспечения, способы изучения

программного обеспечения (статическое и динамическое изучение), временная надежность (невозможность обеспечения гарантированной надежности).

81. Задачи защиты программного продукта от изучения и способы их решений: защита от отладки, динамическое преобразование кода,

82. Итеративный программный замок А. Долгина

83. Принцип ловушек и принцип избыточного кода, защита от дизассемблирования, принцип внешней загрузки файлов, динамическая модификация программы, защита от трассировки по прерываниям.

84. Аспекты защиты от исследования: способы ассоцианирования защиты и программного обеспечения, оценка надежности защиты от отладки.

85. Защита от разрушающих программных воздействий.

86. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия.

87. Понятие изолированной программной среды.

4.4. Шкала оценивания.
4.4.1. Шкала оценивания дисциплины

Набранные баллы	**Оценка**
81-100 баллов	Зачтено / Отлично
61-80 баллов	Зачтено /Хорошо
41-60 баллов	Зачтено/ Удовлетворительно
0-40 баллов и ниже	Неудовлетворительно/Незачтено

Форма текущего контроля и промежуточной аттестации	**Критерии оценивания**	**Максимальный балл**
Практические занятия (аудиторно)	Критерии оценивания устных ответов на вопросы преподавателя по теме занятия и другие виды текущего контроля: правильность и полнота устного ответа согласно плану семинарского занятия, аргументированность позиции в дискуссии.	48
Тестирование (ДОТ)	Три коэффициента веса для тестов разной сложности: тест с ответом да/нет: коэффициент 1Х, тест с ответом 1 из 4: коэффициент 2Х, тест с ответом 3-4 из 6: коэффициент 3Х.	42

Оценка подготовки дискуссии

Параметр	**Оценка (по 5 шкале)**
Выбранная студентом тема (проблема) актуальна на современном этапе развития, представлен подробный план-конспект в котором отражены вопросы для дискуссии, временной регламент обсуждения, даны возможные варианты ответов, использованы примеры из науки и практики	**5**
Выбранная студентом тема (проблема) актуальна на современном этапе развития, представлен содержательно сжатый план-конспект в котором отражены вопросы для дискуссии, временной регламент	**4**

обсуждения, отсутствуют возможные варианты ответов, приведен один пример из практики	
Выбранная студентом тема (проблема) не актуальна на современном этапе развития, представлен содержательно сжатый план-конспект в котором отражены вопросы для дискуссии, отсутствует временной регламент обсуждения, отсутствуют возможные варианты ответов, отсутствуют примеры из практики	**3**
Выбранная студентом тема (проблема) не актуальна на современном этапе развития, представлен содержательно сжатый план-конспект в котором частично (не более 5) отражены вопросы для дискуссии, отсутствует временной регламент обсуждения, отсутствуют возможные варианты ответов, отсутствуют примеры из практики	**2**

Оценка написания эссе по теме

Параметр	**Оценка (по 5 шкале)**
Полученные результаты полностью соответствуют поставленной цели. Обоснована практическая и теоретическая значимость работы. Проведен детальный анализ теоретических и эмпирических источников, выводы автора самостоятельны и аргументированы.	**5**
Полученные результаты преимущественно соответствуют поставленной цели и задачам. Обоснована практическая и теоретическая актуальность работы. В процессе анализа литературы отобран и проанализирован широкий круг теоретических и эмпирических источников.	**4**
Полученные результаты в значительной степени соответствуют поставленной цели (цель работы достигнута в основном). Обоснована актуальность работы.	**3**
Полученные результаты не соответствуют поставленной цели (цель работы достигнута в основном). Обоснована актуальность работы.	**2**

4.4.2. Шкала и критерии оценивания промежуточной аттестации (зачет)

Шкала оценивания по дисциплине	
Баллы	**Критерии оценки**
0-40 (неудовлетворительно)	Студент не знает, либо знает на слабом уровне теоретический материал по дисциплине. Не владеет терминологией и основными понятиями из профессиональной сферы или называет неуверенно, с ошибками.
41-60 (удовлетворительно)	Компетенция освоена удовлетворительно, но достаточно. Студент освоил основную базу теоретических знаний. Владеет терминологией и основными понятиями из профессиональной

	сферы.
61-80 (хорошо)	Студент знает теоретический материал по дисциплине, умеет применить эти знания на практике. Чётко и ясно формулирует свои мысли. Знает специальную и публицистическую литературу по профессиональным вопросам.
81-100 (отлично)	Компетенция освоена в полной мере или на продвинутом уровне. Студент знает теоретический материал, умеет применить эти знания на практике и имеет опыт в профессионально-практической деятельности. Приводит актуальные примеры из сферы профессиональной деятельности; демонстрирует способности к нестандартной интерпретации поставленного вопроса.

5. Методические указания для обучающихся по освоению дисциплины

5.1. Методические указания по самостоятельной подготовке к занятиям практического (лабораторного) типа

Подготовку к каждому практическому/лабораторному занятию каждый студент должен начать с ознакомления с темой занятия. Тщательное продумывание и изучение основывается на проработке текущего материала лекции, а затем изучения обязательной и дополнительной литературы, чтения текстов, выложенных в ДОТ. Если программой дисциплины предусмотрено выполнение задания, то его необходимо выполнить с учетом предложенной инструкции (устно или письменно). Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

В процессе подготовки к занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме.

Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме практического/лабораторного занятия, что позволяет студентам проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

Критерии оценивания устных ответов на вопросы преподавателя по теме занятия - правильность и полнота ответа, аргументированность позиции.

5.2. Методические материалы для подготовки к дискуссии

Дискуссия – это публичный диалог, в процессе которого сталкиваются, как правило, противоположные точки зрения. Дискуссия имеет две основные цели: информационную цель: выявить суть спорного вопроса, четко обозначить все точки зрения; цель воздействия, убеждения: с помощью приведенных аргументов и доказательств убедить соперника в правоте своих взглядов.

При подготовке по теме надо рассмотреть позиции «за» и «против». Каждая позиция должна содержать:

1) определение темы, объяснение ключевых понятий темы;

2) формулировку основного тезиса, с точки зрения которого будет доказываться та или иная позиция;
3) аргументы и доказательства (с опорой на тексты художественной, критической, научной и публицистической литературы).
Успех в дискуссии в значительной степени зависит от аргументов, которые приводятся в поддержку выдвинутого тезиса.
Для ведения продуктивной дискуссии стороны должны уметь задавать информативные и корректные вопросы друг другу.

Прежде чем выступать, надо четко определить свою позицию. Проверить, правильно ли понята суть проблемы. Внимание к выступлению оппонента. Лучшим способом доказательства или опровержения являются бесспорные факты. Лучшим способом убедить противника является четкая аргументация и безупречная логика. Нельзя искажать мысли и слова своих оппонентов.

5.3. Методические рекомендации по написанию эссе

Эссе студента (промежуточная аттестация) - это самостоятельная письменная работа на тему, предложенную преподавателем (тема может быть предложена и студентом, но обязательно должна быть согласована с преподавателем). Цель эссе состоит в развитии навыков самостоятельного творческого мышления и письменного изложения собственных мыслей. Объем эссе – не более 500 слов.

Эссе должно содержать: четкое изложение сути поставленной проблемы, включать самостоятельно проведенный анализ этой проблемы с использованием концепций и аналитического инструментария, рассматриваемого в рамках дисциплины, выводы, обобщающие авторскую позицию по поставленной проблеме.

Эссе состоит из пяти частей (рекомендованные объемы частей написаны в скобках).

1. Реконструкция мысли автора на заданную тему, которая содержит не только формулировку, но и демонстрирует ход рассуждений: посылки, аргументы, вывод. [В текста автор заявляет, что (…), обращаясь к следующим доказательствам …] — [не более 2000 знаков].

2. Критическая позиция студента по поводу мыслей автора, которая содержит обоснование того, почему студент согласен с мыслью автора или нет, обозначение сильных и слабых сторон в его позиции. [Автор утверждает (…), однако с этим сложно согласиться по следующим причинам (…)] — [не более 2000 знаков].

3. Демонстрация своей личной позиции, тезиса, который не может заключаться в простом согласии или несогласии с мнением автора текста — [не более 1000 знаков].

4. Доказательство своего тезиса — [не более 3000 знаков].

5. Заключение, в котором автор кратко сопоставляет свою позицию с позицией автора текста и делает общий вывод по теме уже вне контекста анализируемого текста — [не более 2000 знаков].

Критерии оценивания эссе:

 полнота и точность воспроизведения основных аргументов темы, озвученных в курсе;

 способность к критической рефлексии, обобщению и применению знаний;

 авторский стиль, владение навыками письма и умение формулировать;

 выполнение требований, предъявляемых к эссе.

5.4. Методические рекомендации по выполнению тестовых заданий

Тестирование осуществляется с использованием дистанционных образовательных технологий. Студент самостоятельно выполняет задания к каждой теме. Для выполнения тестового задания, прежде всего, следует внимательно прочитать поставленный вопрос. После ознакомления с вопросом следует приступать к прочтению предлагаемых вариантов ответа. Необходимо прочитать все варианты и в качестве ответа следует выбрать лишь один индекс (цифровое обозначение), соответствующий правильному ответу.

Тесты составлены таким образом, что в каждом из них правильным является как один, так и несколько вариантов. На выполнение теста отводится установленное

ограниченное время. Как правило, время выполнения тестового задания определяется из расчета 30-45 секунд на один вопрос. После выполнения теста происходит автоматическая оценка выполнения. Результат отображается в личном кабинете обучающегося. Повторное прохождение теста допускается не ранее 10 дней.

5.5. Методические рекомендации по самостоятельной работе

Положение об организации самостоятельной работы студентов федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» (в ред. приказа РАНХиГС от 11.05.2016 г. № 01-2211). — URL: http://www.ranepa.ru/images/docs/prikazy-ranhigs/Pologenie_o_samostoyatelnoi_rabote.pdf. Режим свободного доступа.

Виды и формы отработки пропущенных занятий

Студент, пропустивший два занятия подряд, допускается до последующих занятий на основании допуска.

Студент, *пропустивший занятия (одно и более),* отрабатывает каждое из них, сдавая письменное задание по теме реферата на основании литературы к реферату (список литературы и задания предварительно отправляются по электронной почте на адрес группы).

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1.Основная литература

1. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 261 с. — (Высшее образование). — ISBN 978-5-534-01678-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/414082 (дата обращения: 24.01.2021).

6.2.Дополнительная литература

2. Практикум по выполнению лабораторных работ по дисциплине Криптографические методы защиты информации / составители А. Э. Смирнов, Ю. А. Пономарёва. — Москва : Московский технический университет связи и информатики, 2015. — 67 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru.ezproxy.ranepa.ru:3561/61738.html (дата обращения: 29.04.2019). — Режим доступа: для авторизир. пользователей
3. Котов, Ю. А. Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом : учебное пособие / Ю. А. Котов. — Новосибирск : Новосибирский государственный технический университет, 2017. — 67 с. — ISBN 978-5-7782-3411-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru.ezproxy.ranepa.ru:3561/91227.html (дата обращения: 29.04.2019). — Режим доступа: для авторизир. пользователей

6.3.Учебно-методическое обеспечение самостоятельной работы.

4. Креопалов, В. В. Технические средства и методы защиты информации : учебное пособие / В. В. Креопалов. — Москва : Евразийский открытый институт, 2011. — 278 с. — ISBN 978-5-374-00507-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL:

http://www.iprbookshop.ru.ezproxy.ranepa.ru:3561/10871.html (дата обращения: 29.04.2019). — Режим доступа: для авторизир. пользователей
5. Новиков, С. Н. Методы защиты информации : учебное пособие / С. Н. Новиков, О. И. Солонская. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2009. — 121 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru.ezproxy.ranepa.ru:3561/54767.html (дата обращения: 29.04.2019). — Режим доступа: для авторизир. пользователей

6.4. Нормативные правовые документы

6. Доктрина информационной безопасности Российской Федерации.
7. Федеральный закон Российской Федерации «Об информации, информационных технологиях и защите информации» №149-ФЗ от 27 июля 2006 года.
8. Федеральный закон от 4 июля 1996 г. «Об участие в международном информационном обмене».
9. Федеральный закон от 06 апреля 2011 г. N 63-ФЗ "Об электронной подписи".
10. Концепция национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 17 декабря 1997 г. N1300. (В редакции Указа Президента Российской Федерации от 10 января 2000 г. N24.
11. Федеральный закон от 3 февраля 1996 г. N17-ФЗ «О банках и банковской деятельности».
12. Федеральный закон от 22 апреля 1996 г. N39-ФЗ «О рынке ценных бумаг».
13. Федеральный закон от 21 ноября 1996 г. N129-ФЗ «О бухгалтерском учете».
14. Окинавская хартия глобального информационного общества. Принята 22 июля 2000 года. Окинава.
15. Приказ ФСБ РФ №66 от 9 февраля 2005 года «Об утверждении Положения о разработке, производстве, реализации т эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)
16. Указ Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» №351 от 17 марта 2002 года.
17. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
18. ФСТК России. Руководящие документы. М., ФСТК, 2006 г.

6.5. Интернет-ресурсы

19. Официальный сайт ФСТЭК России - 23. [Электронный ресурс]. — URL: http://www.topsbi.com Режим свободного доступа.
20. Билиотека информационных ресурсов по безопасности. [Электронный ресурс]. — URL: http://www.catalog.sec.ru Режим свободного доступа.
21. Портал «Информационная безопасность»: новости, публикации, инновации. [Электронный ресурс]. — URL: http://www.itsec.ru/articles2/allpubliks Режим свободного доступа.

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

7.1. Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Самостоятельная работа (частично) проводятся с использованием дистанционных образовательных технологий.

7.2. Программное обеспечение: Microsoft Windows 10 LTSB 1607, Microsoft Office Professional 2016.

7.3. Информационные справочные системы:

1. Научная библиотека РАНХиГС. URL: http://lib.ranepa.ru/;
2. Научная электронная библиотека eLibrary.ru. URL: http://elibrary.ru/defaultx.asp;
3. Национальная электронная библиотека. URL: www.nns.ru;
4. Российская государственная библиотека. URL: www.rsl.ru;
5. Российская национальная библиотека. URL: www.nnir.ru;
6. Электронная библиотека Grebennikon. URL: http://grebennikon.ru/;
7. Электронно-библиотечная система ЮРАЙТ. URL: http://www.biblio-online.ru/.
8. Электронно-библиотечная система IPR BOOKS. URL: http://www.iprbookshop.