

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

**Институт государственной службы и управления
Кафедра информатики и прикладной математики**

УТВЕРЖДЕНА
решением кафедры информатики
и прикладной математики

Протокол от «26» августа 2019 г. № 1

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**Б1.В.05 Информационная безопасность (Cours Entreprise (Mission) - Interaction between
Authorities and Business in Digital Government. Part 1)**

(индекс, наименование дисциплины, в соответствии с учебным планом)

ИБ

(краткое наименование дисциплины)

38.03.04 Государственное и муниципальное управление

(код, наименование направления подготовки)

**Цифровое государство (российско-французская программа с углубленным изучением
французского языка)**

(направленность (профиль))

бакалавр

(квалификация)

очная

(форма обучения)

2020

(год набора)

Москва, 2019 г.

Авторы–составители:

кандидат экономических наук, доцент, доцент кафедры информатики и прикладной математики Панкратов И.Ю.

кандидат философских наук, доцент, доцент кафедры информатики и прикладной математики Шиловская Е.Е.

Заведующий кафедрой

кандидат технических наук, доцент, исполняющий обязанности заведующего кафедрой информатики и прикладной математики, заместитель директора Института государственной службы и управления Корчагин Р.Н.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы.....	4
2. Объем и место дисциплины в структуре ОП ВО	5
3. Содержание и структура дисциплины.....	5
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине.....	7
5. Методические указания для обучающихся по освоению дисциплины.....	23
6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине.....	24
6.1. Основная литература.....	24
6.2. Дополнительная литература	25
6.3. Учебно-методическое обеспечение самостоятельной работы	25
6.4. Нормативные правовые документы.....	25
6.5. Интернет-ресурсы.....	25
6.6. Иные источники.....	26
7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы	26

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

1.1. Дисциплина Б1.В.05 Информационная безопасность (Cours Entreprise (Mission) - Interaction between Authorities and Business in Digital Government. Part 1) обеспечивает овладение следующими компетенциями с учетом этапа:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ДПК-3	Способность применять современные и актуализирующиеся технологии управления информацией с целью формирования и развития технологических заделов, обеспечение информационной инфраструктурой и информационной безопасности для развития цифрового государства	ДПК – 3.1	Знание и умение применять современные информационно-коммуникационные технологии в области управления информацией для обеспечения развития информационной инфраструктуры цифрового государства.

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

ОТФ/ТФ (при наличии проф- стандарта, или по ре- зультатам форсайт- сессии)	Код этапа освоения компетенции	Результаты обучения
применять современные информационные технологии для описания тенденций развития ключевых институтов (нормативное регулирование, кадры и образование, формирование исследовательских компетенций и технологических заделов) и основных инфраструктурных элементов цифровой экономики (информационная инфраструктура, информационная безопасность)	ДПК – 3.1	на уровне знаний: знает инструментальные средства защиты информации; возможности современных информационных технологий для решения задач информационной безопасности; информационное и программное обеспечение автоматизированных банковских систем; особенности информационной безопасности в профессиональной деятельности; современные подходы к построению систем защиты информации
		на уровне умений: умеет выбрать инструментальные средства для защиты информации и противодействия угрозам в информационной сфере; с помощью программных продуктов обеспечить конфиденциальность, доступность и целостность информационных ресурсов; выбирать рациональные варианты действий в практических задачах обеспечения информационной безопасности; анализировать показатели качества и выбирать критерии оценки систем и отдельных методов и средств защиты информации, в том числе и в

		профессиональной сфере на уровне навыков: владеет навыками работы с основными методами, способами и средствами безопасного получения, хранения, переработки информации; навыки работы с компьютером как средством обеспечения информационной безопасности и как источником основных угроз; применения современных информационно-технических средств защиты информации; работа с пакетом программ, обеспечивающих конфиденциальность, целостность и доступность информации; навыками решения задачи обеспечения информационной безопасности компьютерных систем в профессиональной деятельности
--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

2. Объем и место дисциплины в структуре ОП ВО

Общая трудоемкость Б1.В.05 Информационная безопасность (Cours Entreprise (Mission) - Interaction between Authorities and Business in Digital Government. Part 1) составляет 2 зачетные единицы, 72 часа. Количество академических часов, выделенных на контактную работу с преподавателем, составляет 32 часа: лекционные занятия – 16, лабораторные занятия – 16 часов. Самостоятельная работа составляет 40 часов.

Место дисциплины в структуре ОП ВО

Дисциплина «Информационная безопасность» (Cours Entreprise (Mission) - Interaction between Authorities and Business in Digital Government. Part 1) относится к дисциплинам вариативной части Блока 1 «Дисциплины (модули)» и изучается на 4 курсе (7 семестр).

Содержание дисциплины является продолжением содержания курсов Б1.Б.09.02 Информационные технологии в государственном и муниципальном управлении (1 семестр), Б1.В.19.01 Информационные системы (European Logistic Management. Part 2) (6 семестр), Б1.В.12 Системы управления базами данных (4 семестр).

Форма промежуточной аттестации в соответствии с учебным планом – зачет (7 семестр).

3. Содержание и структура дисциплины

Очная форма обучения

№ п/п	Наименование тем (разделов)	Объем дисциплины (модуля), час.					СР	Форма текущего контроля успеваемости*, промежуточной аттестации**
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий					
			Л	ПЗ	ЛР	КСР		
Тема 1	Основные понятия информационной безопасности и защиты информации	8	2		2		4	О
Тема 2	Угрозы информационной безопасности	8	2		2		4	О, КР
Тема 3	Политика информационной безопасности	8	2		2		4	О

№ п/п	Наименование тем (разделов)	Объем дисциплины (модуля), час.					СР	Форма текущего контроля успеваемости*, промежуточной аттестации**
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий					
			Л	ПЗ	ЛР	КСР		
Тема 4	Правовые основы обеспечения информационной безопасности	8	2		2		4	О
Тема 5	Стандарты обеспечения информационной безопасности	8	2		2		4	О
Тема 6	Безопасность операционных систем	12	2		2		8	О, КР
Тема 7	Криптографическая защита информации	12	2		2		8	О, Т, КР
Тема 8	Защита от вредоносных программ и спама	8	2		2		4	О
Промежуточная аттестация								За
Всего:		72	16		16		40	

Примечание:

* - формы текущего контроля успеваемости: опрос (О), тестирование (Т), контрольная работа (КР), задачи (З)

** - формы промежуточной аттестации: зачет (За).

Содержание дисциплины

Тема 1. Основные понятия информационной безопасности и защиты информации.

Основные понятия. Понятие информационной безопасности. Основные свойства информационной безопасности. Информационные риски и безопасность информации. Анализ информационных рисков. Особенности информации как объекта защиты. Защищенные информационные системы. Организация работы в защищенных системах.

Тема 2. Угрозы информационной безопасности.

Классификация угроз информационной безопасности. Случайные и преднамеренные угрозы. Характеристика физических каналов негативного воздействия на информационные ресурсы и его последствий. Технологические возможности злоумышленников по преодолению систем защиты информации.

Тема 3. Политика информационной безопасности.

Значение организационного обеспечения информационной безопасности. Понятие политики информационной безопасности. Комплексный подход к обеспечению информационной безопасности. Задачи комплексной защиты обеспечения информационной безопасности. Принципы обеспечения ИБ БС РФ (общие и специальные). Основные объекты защиты с точки зрения информационной безопасности в государственных учреждениях. Основные разделы политики информационной безопасности. Основные категории специализированных политик безопасности. Недостатки приложений дистанционного банковского обслуживания и электронных средств платежа.

Тема 4. Правовые основы обеспечения информационной безопасности.

Государственная политика РФ в области правового обеспечения информационной безопасности. Особенности информации как объекта права. Законодательство РФ в сфере информационных технологий. Структура государственных органов РФ, осуществляющих правотворчество и правоприменение в области информационной безопасности. Понятия государственной, коммерческой и служебной тайны.

Тема 5. Стандарты обеспечения информационной безопасности.

Стандарты и рекомендации в области защиты информации. Критерии защищенности компьютерных систем. Стандарт BS 7799:2005. Стандарт ИСО 27001. Стандарты для беспроводных сетей. Отечественные стандарты информационной безопасности. Основные стандарты Банка России в части обеспечения информационной безопасности. Стандарт PCI DSS.

Тема 6. Безопасность операционных систем.

Защита информации в компьютерных системах от несанкционированного доступа. Система разграничения доступа к информации. Противодействие несанкционированному изучению и использованию программного обеспечения.

Методы и средства защиты от несанкционированного изменения структур компьютерных систем. Методы контроля целостности информации. Доверенная загрузка операционных систем. Защита от несанкционированного доступа к внутреннему монтажу и средствам коммутации, от подключения нештатных устройств. Системы защиты от несанкционированного доступа к ПК.

Средства ОС и MS Office по защите от несанкционированного доступа к документам.

Тема 7. Криптографическая защита информации.

Основные понятия криптографии. Криптографические методы защиты информации. Методы стеганографии. Классификация методов шифрования. Требования к современным шифрам. Методы симметричного шифрования. Блочное и потоковое шифрование. Абсолютно надежный шифр. Несимметричное шифрование.

Применение методов криптографии для идентификации и аутентификации удаленных процессов. Цифровая электронная подпись. Перспективы развития криптографии.

Тема 8. Защита от вредоносных программ и спама.

Защита информации в каналах связи. Межсетевое экранирование. Подтверждение подлинности информации и взаимодействующих процессов.

Обеспечение информационной безопасности процессов функционирования систем электронной торговли и дистанционного банковского обслуживания клиентов.

Методы и средства обеспечения безопасной работы в глобальной сети Интернет.

Классификация компьютерных вирусов и вредоносных программ. Файловые, загрузочные и сетевые вирусы. Методы и средства борьбы с вирусами и вредоносными программами. Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения

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

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

4.1.1. В ходе реализации дисциплины Б1.В.05 Информационная безопасность (Cours Entreprise (Mission) - Interaction between Authorities and Business in Digital Government. Part 1) используются следующие методы текущего контроля успеваемости обучающихся:

Тема (раздел)		Формы (методы) текущего контроля успеваемости
Тема 1	Основные понятия информационной безопасности и защиты информации	Опрос
Тема 2	Угрозы информационной безопасности	Опрос, контрольная работа
Тема 3	Политика информационной безопасности	Опрос
Тема 4	Правовые основы обеспечения информационной	Опрос

	безопасности	
Тема 5	Стандарты обеспечения информационной безопасности	Опрос
Тема 6	Безопасность операционных систем	Опрос
Тема 7	Криптографическая защита информации	Опрос, контрольная работа, тестирование
Тема 8	Защита от вредоносных программ и спама	Опрос

4.1.2. Зачет проводится с применением следующих методов (средств): в устной форме.

4.2. Материалы текущего контроля успеваемости.

Преподаватель оценивает уровень подготовленности обучающихся к занятию по следующим показателям:

- устные ответы на вопросы преподавателя по теме занятия,
- решение практических задач,
- выполнение контрольных работ.

Оценка знаний, умений, навыков проводится на основе балльно-рейтинговой системы 70% из 100% (70 баллов из 100) - вклад по результатам посещаемости занятий, активности на занятиях, решение практических задач на семинарских занятиях, ответов на вопросы преподавателя в ходе занятия, по результатам выполнения домашних контрольных работ.

Вопросы для подготовки к опросам, лабораторным занятиям по темам:

Тема 1 Основные понятия информационной безопасности и защиты информации.

1. Что такое информационная безопасность в соответствии с Доктриной ИБ 2016 г. ?
2. Как Банк России понимает информационную безопасность?
3. Что в соответствии с международными стандартами понимается под термином «информационная безопасность»
4. Что понимается под термином национальные интересы Российской Федерации в информационной сфере?
5. Назовите хотя бы один национальный интерес РФ в информационной сфере.
6. Мы говорили о КЦД подходе к информационной безопасности. Что такое КЦД?
7. Что такое конфиденциальность в аспекте обеспечения информационной безопасности?
8. Что такое целостность в аспекте обеспечения информационной безопасности?
9. Что такое доступность в аспекте обеспечения информационной безопасности?
10. Мы говорили о нескольких подходах к пониманию информационной безопасности. Какой подход содержится в резолюции ООН «Создание глобальной культуры кибербезопасности»? Назовите основные принципы этого подхода.
11. Что собой подразумевает экономический подход к пониманию информационной безопасности?
12. Что такое защита информации?
13. Что из себя представляет система информационной безопасности?
14. Что такое угроза информационной безопасности в соответствии с Доктриной ИБ 2016 г.?
15. Чем термин уязвимость отличается от такого понятия как угроза?
16. Назовите одну-две угрозы информационной безопасности в соответствии с Доктриной ИБ.

17. Мы рассматривали отчеты компании PWC. Какое место среди экономических преступлений занимает киберпреступность.
18. Как вы понимаете термин «киберпреступление»?
19. Назовите основные направления воздействия киберпреступлений на бизнес компании.
20. Объясните, пожалуйста, следующую фразу «кибербезопасность - это не только технический риск, это бизнес риск».
21. Какие сферы наиболее привлекательны для киберпреступников.

Тема 2. «Угрозы информационной безопасности»

1. Что такое угроза информационной безопасности в соответствии с Доктриной ИБ 2016 г.?
2. Чем термин уязвимость отличается от такого понятия как угроза?
3. Что из себя представляет первичная классификация угроз информационной безопасности?
4. Что из себя представляют угрозы нарушения доступности (целостности, конфиденциальности) информации?
5. Каким образом классифицируются угрозы ИБ по степени воздействия на информационную систему?
6. Дайте, пожалуйста, краткую характеристику атакам типа АРТ. Приведите примеры таких атак.
7. Назовите основные типы вредоносных программ.
8. Какие типы вредоносных программ занимают лидирующее положение по степени распространенности?
9. Назовите основные подходы к классификации сетевых атак.
10. Назовите типы сетевых атак по цели воздействия. Что из себя представляют атаки доступа (модификации, отказа в обслуживании)?
11. Назовите основные виды сетевых атак доступа. Что такое перехват (прослушивание канала, подмена доверенного хоста, навязывание пакетов)?
12. Назовите основные виды сетевых атак отказа в обслуживании.
13. Какие комбинированные атаки вы знаете? Что из себя представляет атака подмена доверенного субъекта (атака человек посередине, атака DNS-spoofing)?
14. Какие интернет-атаки вы знаете? Что из себя представляет фарминг(фишинг, инъекция кода)?
15. Что такое ботнеты и для чего они используются.
16. Что из себя представляют шифровальщики?
17. Назовите основные виды атак на WIFI-сети (взлом WPA-паролей, замена точки доступа фальшивой, отказ в обслуживании)
18. Что из себя представляет атака water-holing
19. Назовите типичные недостатки Интернет-банков.
20. Что такое двухфакторная аутентификация?
21. Как вы понимаете возможность дублирования сессии в Интернет-банке.

Контрольная работа №1

ВАРИАНТ 1

I. Задание 1. У Гражданина А пропала сеть на телефоне, на котором был зарегистрирован мобильный банк. Позвонив сотовому оператору, он узнал о незаконном выпуске SIM-карты. Затем получив доступ к своему банковскому счету, узнал, что с дебетовой карты было похищено 450 000р. Также исчезли деньги с банковского депозита.

1. Сформулируйте интересы клиента банка, которые были нарушены в данном условии.
2. Перечислите угрозы интересам клиента банка, характерные для данного задания.

3. Назовите основные объекты и субъекты системы обеспечения информационной безопасности, затронутые в данном задании?

4. Перечислите возможные каналы и способы доступа к банковскому счету клиента с целью хищения денежных средств, используемые злоумышленниками в данном задании.

5. Классифицируйте тип атаки мошенников для этого задания.

6. Назовите основные причины (уязвимости) проведения атаки в данном задании.

7. Назовите банки (отечественные и зарубежные), принявшие специальные меры в части проверки перевыпуска sim-карты.

8. Перечислите мероприятия, необходимые для предотвращения таких ситуаций (подобных ситуации в задании, как со стороны клиента, так и со стороны банка.

II. Как, по-вашему, изменятся подходы к обеспечению информационной безопасности в банковской сфере в ближайшие 5-10 лет?.

ВАРИАНТ 2

I. Задание 2. Приходит СМС /БАНК/Заявка на перевод 12000 руб. с вашей карты принята. Инф. 8(904)9383439. Гражданин Б, поскольку у него включена услуга «Мобильный банк» принял сообщение, позвонил по указанному телефону и сделал продиктованные злоумышленником действия с картой. В результате - потеря довольно большой суммы с карты.

1. Сформулируйте интересы клиента банка, которые были нарушены в данном задании.

2. Перечислите угрозы интересам клиента банка, характерные для данного задания.

3. Назовите основные объекты и субъекты системы обеспечения информационной безопасности, затронутые в данном задании?

4. Перечислите возможные каналы и способы доступа к банковскому счету клиента с целью хищения денежных средств, используемые злоумышленниками в данном задании.

5. Классифицируйте тип атаки мошенников для этого задания.

6. Назовите основные причины (уязвимости) проведения атаки в данном задании.

7. Перечислите основные отличия «фишинга» от «фарминга»?

8. Перечислите мероприятия, необходимые для предотвращения таких ситуаций (подобных ситуации в задании), как со стороны клиента, так и со стороны банка.

II. Какие, по-вашему, новые аппаратно-программные коммуникационные технологии появятся (хотели бы чтобы появились) в сфере обеспечения информационной безопасности в банковской сфере в ближайшие пять-семь лет?

Тема 3. Политика информационной безопасности.

1. Что такое политика информационной безопасности?

2. Какие существуют подходы к обеспечению информационной безопасности?

3. Расскажите про сущность и содержание фрагментарного (комплексного) подхода к обеспечению информационной безопасности.

4. Какие бывают меры по обеспечению информационной безопасности (законодательные, программно-технические, административно-организационные)?

5. Что включают в себя законодательные (программно-технические, административно-организационные) меры по обеспечению информационной безопасности?

6. Назовите две-три задачи комплексной защиты обеспечения информационной безопасности.

7. Назовите основные категории принципов обеспечения ИБ БС РФ (общие и специальные)

8. Что из себя представляет Принцип «Знать своего клиента» (Принцип «Знать своего служащего», Принцип «Необходимо знать»)?
9. Что такое PDCA-цикл (цикл Деминга) и особенности его применения при формировании системы обеспечения информационной безопасности.
10. Назовите основные объекты защиты с точки зрения информационной безопасности в Банке
11. Назовите основные разделы политики информационной безопасности.
12. Какие бывают уровни политик информационной безопасности (верхний, средний и нижний)
13. Назовите основные категории специализированных политик безопасности
14. В чем заключается сущность и содержание политики допустимого использования (политики удаленного доступа)?
15. В чем заключается сущность и содержание процедур безопасности? Какие бывают процедуры ?
16. Назовите основные шаги по разработке политики безопасности (анализ рисков, анализ требований бизнеса)
17. Назовите основные компоненты физической безопасности (логической безопасности)
18. Что такое аудит информационной безопасности? Какие аспекты аудита информационной безопасности необходимо учитывать?
19. Назовите два-три недостатка веб-приложений при доступе к личным данным (управления сессиями, размещение компонентов веб-приложения)
20. Назовите два-три недостатка приложений дистанционного банковского обслуживания и электронных средств платежа (безопасность транзакций)
21. Назовите два-три недостатка операционных систем (идентификация и аутентификация, управление доступом)
22. Перечислите три самых распространенных уязвимостей систем ДБО (недостаточная авторизация, недостаточная защита сессии, идентификация приложения)

Тема 4. Правовые основы обеспечения информационной безопасности.

1. Что включает в себя нормативное и правовое обеспечение информационной безопасности РФ?
2. Что подразумевает комплексный подход к обеспечению информационной безопасности?
3. Перечислите две-три нормы, положения Конституции РФ в части обеспечения информационной безопасности.
4. Какая роль информационной безопасности отведена в Стратегии развития информационного общества РФ?
5. Каким образом отражена проблема информационной безопасности в Стратегии национальной безопасности РФ?
6. В Стратегии национальной безопасности есть такой термин стратегический национальный приоритет. Что это такое?
7. Какова структура Доктрины информационной безопасности от 2016 года?
8. Какие две-три угрозы национальной безопасности в информационной сфере в соответствии с Доктриной ИБ 2016 года?
9. В чем заключается обеспечение информационной безопасности в экономической сфере?
10. В чем заключается обеспечение информационной безопасности в области науки, технологий и образования?
11. Перечислите основные субъекты обеспечения информационной безопасности в РФ?

12. Сущность и содержание принципов обеспечения информационной безопасности РФ. Назовите два-три из них.
13. Предусмотрена ли уголовная ответственность за преступления, связанные с информационной безопасностью. Назовите конкретные статьи УК РФ;
14. В каких Кодексах РФ имеются положения, регулирующие правоотношения в сфере обеспечения информационной безопасности?
15. Предусмотрена ли административная ответственность за правонарушения, связанные с информационной безопасностью. Назовите конкретные статьи КОАП РФ?
16. Назовите цель Федерального закона «Об информации, информационных технологиях и о защите информации»? Какие статьи регулируют отношения в сфере обеспечения информационной безопасности.
17. Назовите цель Закона «О банках и банковской деятельности» Какие статьи посвящены проблеме обеспечения ИБ
18. Назовите Цель и раскройте содержание Федерального закона «о Национальной платежной системе»
19. Какие нормативные документы существуют в сфере обеспечения информационной безопасности? Правительство РФ и ЦБ РФ

Тема 5. Стандарты обеспечения информационной безопасности.

1. Что такое стандарты информационной безопасности.
2. Назовите основные функции стандартов информационной безопасности?
3. Назовите основную задачу стандартов информационной безопасности?
4. В чем интерес потребителей (производителей и экспертов) при использовании (разработке) продукта в части информационной безопасности.
5. Каким образом классифицируют стандарты (критерии классификации)?
6. Из скольких частей состоит стандарт BS 7799:2005?
7. В чем заключается четырехфазная модель процесса управления информационной безопасностью согласно стандарту BS 7799:2005?
8. Что составляет основу стандарта ИСО 27001?
9. Опишите структуру стандарта ИСО 27001?
10. Какие стандарты для беспроводных сетей вы знаете?
11. Какие стандарты безопасности для Интернета вы знаете.
12. Для чего предназначен протокол SET?
13. Какие отечественные стандарты информационной безопасности вы знаете?
14. Назовите основные части стандарта ГОСТ Р ИСО/МЭК 15408?
15. Назовите основные стандарты Банка России в части обеспечения информационной безопасности?
16. Какой стандарт в части информационной безопасности Банк России принял в конце 2016 года?
17. Назовите основные требования к обеспечению информационной безопасности в соответствии со стандартом СТО БР ИББС-1.0-2014. «Общие положения»;
18. Назовите основную цель и задачи стандарта Банка России «Методика оценки соответствия требованиям ИБ»;
19. О чем стандарт PCI DSS?
20. Назовите основные группы данных в соответствии со стандартом PCI DSS?
21. Назовите основные группы показателей в соответствии с «Методикой оценки соответствия требованиям ИБ»
22. Сколько уровней для каждого показателя предусмотрено стандартом БР «Методика оценки соответствия требованиям ИБ»?

Тема 6. Безопасность операционных систем.

1. Назовите основные критерии классификации угроз безопасности операционной системы?
2. Что такое программная закладка?
3. Назовите типичные атаки на операционную систему. Что из себя представляет сборка мусора? (жадные программы)
4. Назовите обязательные составляющие защищенной операционной системы
5. Назовите основные подходы к построению защищенных операционных систем
6. Перечислите основные функции подсистемы защиты операционной системы
7. Назовите основные методы идентификации и аутентификации в ОС
8. Что Вы понимаете под термином «разграничение доступа»
9. Кто такой суперпользователь?
10. Назовите основные модели разграничения доступа
11. Что такое матрица доступа?
12. Назовите преимущества и недостатки модели избирательного разграничения доступа.
13. Чем изолированная программная среда отличается модели избирательного разграничения доступа
14. В чем заключается аудит в операционной системе?
15. Назовите некоторые недостатки операционных систем, связанных с управлением доступом (идентификацией и аутентификацией, управления системой)
16. Какие средства защиты Windows 8 вы знаете?
17. Для чего нужны bitlocker и bitlocker to go и в чем их различия?
18. Какая система шифрования существует в ОС WINDOWS 8;
19. Для чего нужна служба управления правами в Windows 8?
20. Назовите основные составляющие службы управления правами в Windows 8.
21. Что такое брандмауэр Windows 7 и какие основные профили он предусматривает?
22. Для чего используется технология AppLocker?

Задание

1. Создайте нового пользователя temp1 с паролем «12345» и добавьте его в группу «Криптографические операторы».
2. Исключите пользователя temp из группы «Операторы помощи по контролю учетных записей»;
3. Отключите встроенную учетную запись «Гость»
4. Для пользователя Ivanov для указанной папки: А) разрешить «Чтение и выполнение»; Б) Запретить «Запись».
5. С помощью утилиты BitLocker To Go защитите съемный носитель;
6. С помощью брандмауэра Windows 8 заблокируйте исходящие подключения к 80-му порту (HTTP) для профиля «Частный» для всех пользователей;
7. С помощью брандмауэра Windows 8 разрешите все входящие подключения для программы Skype для профиля «Частный» и только для пользователя Ivanov (skype_rules);
8. С помощью системы EFS зашифруйте указанный файл;
9. Откройте файл update.docx используя пароль stadium. Удалите пароль на открытие файла и вставьте пароль 12345 для возможности редактирования файла;
10. Откройте файл rainbow.xlsx. Защитите только диапазон ячеек C20:D20 используя пароль «12345». Гарантируйте, что все другие ячейки на рабочем листе доступны для редактирования.
11. С помощью Applocker создайте стандартные правила (Default rules) для запуска приложений
12. С помощью Applocker создайте запретительное правило для пользователя temp для приложения Skype.exe.

13. С помощью Applocker создайте разрешительное правило для запуска упакованного приложения Магазин только от пользователя Ivanov;
14. Назовите два последних события из журнала безопасности Windows 8;
15. В центре поддержки Windows отключите сообщения безопасности (обновление Windows, Брандмауэр)
16. Включить возможность выполнения операционной системой Windows 8 аудита каждой попытки входа пользователя в систему или выхода из нее.

Тема 7. Криптографическая защита информации.

1. Что такое Криптография?
2. Назовите основные функции криптографической защиты информации
3. Что такое шифр?
4. Какие бывают криптоалгоритмы?
5. Что такое хэширование?
6. Что такое симметричное шифрование?
7. Что такое асимметричное шифрование?
8. Чем блочное шифрование отличается от поточного?
9. Для чего нужна матрица ключей в симметричных алгоритмах шифрования?
10. Идеально стойкий криптоалгоритм – этой какой?
11. Основные свойства и качества алгоритма DES
12. Основные преобразования в алгоритме AES
13. Какие симметричные алгоритмы вы знаете?
14. Объясните принцип работы симметричных криптоалгоритмов
15. Назовите основные недостатки симметричного шифрования
16. Какие ключи используются в асимметричных алгоритмах шифрования?
17. Назовите преимущества асимметричных шифров перед симметричными?
18. Назовите основные недостатки асимметричных шифров
19. Назовите известные алгоритмы асимметричного шифрования
20. Что такое факторизация числа
21. Объясните принцип работы асимметричных криптоалгоритмов
22. Объясните принцип работы хэшфункции
23. Назовите основные функции хэшфункции
24. Назовите известные функции хэширования
25. Для чего используется электронная цифровая подпись
26. Назовите основные процедуры ЭЦП
27. Объясните принцип действия процедуры формирования цифровой подписи
28. Объясните принцип действия процедуры проверки цифровой подписи
29. Какую информацию содержит ЭЦП?
30. Объясните принцип действия комбинированного применения симметричного и асимметричного шифрования

Вопросы к тестированию (образец)

1. В соответствии с Доктриной информационной безопасности РФ от 5 декабря 2016 года информационная безопасность это:
 - А) состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз;
 - Б) защищенность информации от незаконного ознакомления, преобразования и уничтожения;
 - В) деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемый объект.
 - г) система официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

д) состояние защищенности интересов государства от внутренних и внешних информационных угроз

е) состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере

2. Для киберпреступлений характерны:

А) **Высокая латентность;**

Б) Наличие достаточной следственной практики по раскрытию компьютерных преступлений в РФ;

В) Простота сбора доказательств;

Г) Излишне жесткие санкции

Д) **Киберпространство - это источник, инструмент, цель или место преступления**

Е) **использование электронных носителей и устройств является основным , а не случайным элементом;**

Ж) **отсутствие детализации составов киберпреступлений в РФ**

3. Недостатками Интернет-банков являются:

А) Отсутствие проверки перевыпуска SIM карты;

Б) **Отсутствие двухфакторной аутентификации;**

В) **Возможность дублирования сессии;**

Г) Возможность доступа к операционной системе без аутентификации через вспомогательные и (или) редко используемые интерфейсы (serial-порты и т.п.)

Д) Совместное расположение журналов регистрации событий и системных файлов

Е) Очень строгая парольная политика

4. Назовите ключевые свойства информационной безопасности:

А) Конфиденциальность, целостность, актуальность;

Б) Полнота, достоверность, целостность;

В) **Доступность, конфиденциальность, целостность;**

Г) Конфиденциальность, доступность, актуальность.

Д) Доступность, целостность, защищенность;

Е) Целостность, конфиденциальность, защищенность;

Ж) Защищенность, непротиворечивость, доступность

5. Атакой на автоматизированные банковские системы и системы ДБО не является:

А) **Аутсорсинг;**

Б) Прослушивание канала;

В) Подмена доверенного хоста

Г) Фарминг;

Д) **Краудфайдинг;**

Е) IP-SPOOFING

Ж) PHP-инъекция

6. В соответствии с подходами Центрального Банка РФ информационная безопасность это:

А) состояние защищенности национальных интересов РФ в информационной сфере;

Б) защищенность информации БС РФ от незаконного ознакомления, преобразования и уничтожения;

В) **состояние защищенности интересов - целей организации БС РФ в условиях угроз в информационной сфере;**

- Г) деятельность ЦБ РФ по предотвращению утечки защищаемой информации, не-санкционированных и непреднамеренных воздействий на защищаемый объект;
- Д) состояние защищенности банковских интересов РФ в информационной сфере;
- Е) защищенность ЦБ РФ от угроз в информационной сфере

7. По цели воздействия сетевые атаки бывают:

- А) Атаки доступа;**
- Б) Атаки модификации;**
- В) Активные атаки
- Г) Пассивные атаки
- Д) Атаки отказа в обслуживании**
- Е) Сложные атаки

8. Выберите два сектора, наиболее привлекательных для киберпреступников:

- А) Финансовые услуги и страхование;**
- Б) Нефтегазовый сектор;
- В) Государство;
- Г) Система образования
- Д) Фармацевтика и химическое производство;**
- Е) ИТ, телеком и медиа

9. Что не относится к угрозам информационной безопасности:

- А) классификация информации;**
- Б) сбои и отказы оборудования (технических средств);
- В) преднамеренные действия нарушителей и злоумышленников.
- Г) Удаление не нужной информации**
- Д) Дефрагментация жестких дисков;**
- Е) Перехват информации;
- Ж) Установка антивирусного программного обеспечения**

10. Перехват сеанса это -:

- А) Возможность злоумышленника, получившего доступ к линиям передачи данных в вашей сети, подслушивать или считывать трафик;
- Б) Злоумышленник захватывает информацию в процессе ее передачи к месту назначения;

В) По окончании начальной процедуры аутентификации соединение, установленное законным пользователем, например с почтовым сервером, переключается злоумышленником на новый хост.

Г) Атака, направленная против информации, когда последняя становится непригодной для использования;

Д) перенаправление пользователей на фальшивые сайты, являющиеся копиями оригинальных

11. Конфиденциальность – это:

А) свойство информации, при котором предоставляется возможность за приемлемое время получить требуемую информационную услугу;

Б) состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

В) свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц

Г) свойство ИБ, при котором обеспечивается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Д) защищенность информации от незаконного ознакомления, преобразования и уничтожения

Е) свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц ;

Ж) неизменность информации в процессе ее передачи или хранения, избежание не-санкционированной модификации информации

12. В соответствии с подходами ЦБ РФ угроза информационной безопасности - это:

А) угроза нарушения свойств информационной безопасности ;

Б) совокупность условий или действий, создающих потенциальную или реально существующую опасность нарушения безопасности информации;

В) совокупность условий и факторов, препятствующих реализации целей БС РФ;

Г) совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере;

Д) совокупность условий и факторов, препятствующих реализации интересов личности и общества в банковской сфере РФ

Е) совокупность условий и факторов, обуславливающих возможность реализации уязвимости информационной системы в БС РФ

13. Выберите два типа зловредного ПО, на которых, в основном, сосредоточены новые разработки

А) трояны;

Б) вирусы;

в) сетевые черви;

г) шпионы и рекламное ПО;

д) программы нежелательного поведения;

14. Что из себя представляет атака «water holing»:

А) нападавшие определяют и заражают кластер сайтов, который по их мнению посетят члены целевой организации;

Б) вывод из строя компьютерной системы, в результате чего сама система, установленные на ней приложения и вся сохраненная информация становятся недоступными.

В) захват информации в процессе ее передачи к месту назначения.

Г) блокировка доступа пользователей к файлам на компьютере с использованием шифрования;

Д) злоумышленник, находящийся внутри корпорации или вне ее, выдает себя за законного пользователя

15. Сотрудники каких отделов в банках отмечают существенный рост угроз информационной безопасности в ближайшее время:

А) Отдел казначейства;

Б) Отдел аудита;

В) Отдел рисков.

Г) Топ-менеджеры

16. Какая из следующих угроз информационной безопасности связана с облачными вычислениями?

А) Не обеспечен должный контроль за файлами cookie на жестком диске.

Б) Затруднен доступ к устройствам хранения музыки на мобильном устройстве.

В) Взлом данных на диске USB.

Г) Потенциальная потеря контроля за онлайн-файлами.

Д) угроза удаленного взлома или заражения вредоносным ПО

17. Вы думаете, что были подвержены попытке кражи личных данных, на основании того, что слот для банковской карты на АТМ-устройстве выглядел не совсем обычно. Какой способ кражи личных данных мог быть использован злоумышленником?

- А) Фишинг
- Б) Подслушивание
- В) Претекстинг
- Г) **Скимминг**
- Д) Сриннинг
- Е) Кейлоггинг

18. Какой из следующих паролей является примером хорошей парольной политики?

- А) 12061985
- Б) password1.
- В) **w1g_w@ms.**
- Г) access.

19. В соответствии с подходами ЦБ России политика информационной безопасности – это:

- А) Состояние защищенности интересов (целей) организации БС РФ в условиях угроз в информационной сфере
- Б) Свойство ИБ организации БС РФ сохранять неизменность или исправлять обнаруженные изменения в своих информационных активах
- В) **Документация, определяющая высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ, предназначенная для организации БС РФ в целом;**
- Г) Обязательные или рекомендуемые к выполнению документы, в которых определены подходы к оценке уровня ИБ и установлены требования к безопасным информационным системам;
- Д) деятельность ЦБ РФ по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемый объект;
- Е) состояние защищенности банковских интересов РФ в информационной сфере

20. Что из нижеследующего лучше всего описывает принцип «Знать своего клиента»?

- А) принцип безопасности, который ограничивает доступ к информации и ресурсам по обработке клиентской информации;
- Б) **принцип, используемый регулирующими органами для выражения отношения к финансовым организациям с точки зрения знания деятельности их клиентов**
- В) принцип, демонстрирующий озабоченность организации по поводу отношения клиентов к обеспечению информационной безопасности;
- Г) принцип сохранения целостности процесса и борьбы с искажением функций системы, требующий того, чтобы два лица независимо предпринимали некое действие до завершения определенных транзакций
- Д) принцип безопасности, который ограничивает доступ к информации и ресурсам по обработке информации тем, кому требуется выполнять определенные обязанности

Контрольная работа №2
ВАРИАНТ 1

I. Комплексный подход к решению проблемы обеспечения информационной безопасности заключается в рациональном сочетании законодательных, административно-организационных и программно-технических мер и механизмов. Сделайте обобщающие выводы в части соответствия законодательных (нормативных и правовых) мер современным вызовам и угрозам в сфере обеспечения информационной безопасности Российской Федерации.

II. Вы изучили набор инструментов для защиты данных в операционных системах Windows. Какие из них Вы планируете использовать в будущем? И как их можно сделать более удобными в использовании?

III. Вас назначили начальником отдела информационной безопасности в Сбербанк. Сформулируйте основные Ваши рекомендации и предложения в части совершенствования системы обеспечения информационной безопасности компании, исходя из корпоративных интересов и приоритетов ее деятельности.

ВАРИАНТ 2

I. Комплексный подход к решению проблемы обеспечения информационной безопасности заключается в рациональном сочетании законодательных, административно-организационных и программно-технических мер и механизмов. Сделайте обобщающие выводы в части соответствия административно-организационных мер современным вызовам и угрозам в сфере обеспечения информационной безопасности Российской Федерации.

II. Вы изучили набор инструментов для защиты данных в операционных системах Windows. Сделайте обоснованный вывод об их достаточности в части защиты данных в операционной системе и предложите свои рекомендации, касающиеся разработки новых механизмов и инструментов, а также совершенствования имеющихся.

III. Вас назначили начальником отдела информационной безопасности в соответствующем Департаменте Министерства Финансов РФ. Сформулируйте основные Ваши задачи и полномочия на этом ответственном посту.

Тема 8. Защита от вредоносных программ и спама

1. Что вы понимаете под термином «вредоносное программное обеспечение»?
2. Классификация вредоносных программ
3. Назовите основные отличительные характеристики компьютерных вирусов, сетевых червей и троянских программ
4. Классификация троянских программ и сетевых червей
5. Основные режимы работы антивирусных программ
6. Недостатки и преимущества сигнатурного анализа
7. Недостатки и преимущества эвристического анализа
8. Основные модули антивирусов
9. Как работают антивирусные облака?
10. Основные продукты Лаборатории Касперского.

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 компе-	Наименование	Код этапа освое-	Наименование этапа освое-
------------	--------------	------------------	---------------------------

тенции	компетенции	ния компетенции	ния компетенции
ДПК-3	Способность применять современные и актуализирующиеся технологии управления информацией с целью формирования и развития технологических заделов, обеспечение информационной инфраструктурой и информационной безопасности для развития цифрового государства	ДПК –3.1	Знание и умение применять современные информационно-коммуникационные технологии в области управления информацией для обеспечения развития информационной инфраструктуры цифрового государства.

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
ДПК-3.1 Знание и умение применять современные информационно-коммуникационные технологии в области управления информацией для обеспечения развития информационной инфраструктуры цифрового государства.	Знает правила, методы получения, обработки и анализа информации, в том числе с использованием современных информационно-коммуникационных технологий	Всесторонне знает правовые основы, правила, методы получения, обработки и анализа информации

4.3.2 Типовые оценочные средства

Вопросы к зачету

1. Что такое информационная безопасность в соответствии с Доктриной ИБ 2016 г. ?
2. Что понимается под термином национальные интересы Российской Федерации в информационной сфере?
3. Что такое доступность в аспекте обеспечения информационной безопасности?
4. Что такое защита информации?
5. Что такое угроза информационной безопасности в соответствии с Доктриной ИБ 2016 г.?
6. Какие сферы наиболее привлекательны для киберпреступников.
7. Какие комбинированные атаки вы знаете? Что из себя представляет атака подмена доверенного субъекта (атака человек посередине, атака DNS-spoofing)
8. Какие интернет-атаки вы знаете? Что из себя представляет фарминг(фишинг, инъекция кода)?
9. Назовите типичные недостатки Интернет-банков.
10. Что такое двухфакторная аутентификация?
11. Как вы понимаете возможность дублирования сессии в Интернет-банке.
12. Что такое политика информационной безопасности?
13. Какие существуют подходы к обеспечению информационной безопасности?

14. Назовите основные категории принципов обеспечения ИБ БС РФ (общие и специальные)
15. Что из себя представляет Принцип «Знать своего клиента» (Принцип «Знать своего служащего», Принцип «Необходимо знать»)?
16. Что такое PDCA-цикл (цикл Деминга) и особенности его применения при формировании системы обеспечения информационной безопасности.
17. Назовите основные шаги по разработке политики безопасности (анализ рисков, анализ требований бизнеса)
18. Назовите основные компоненты физической безопасности (логической безопасности)
19. Что такое аудит информационной безопасности? Какие аспекты аудита информационной безопасности необходимо учитывать?
20. Что включает в себя нормативное и правовое обеспечение информационной безопасности РФ?
21. Какова структура Доктрины информационной безопасности от 2016 года?
22. В каких Кодексах РФ имеются положения, регулирующие правоотношения в сфере обеспечения информационной безопасности?
23. Предусмотрена ли административная ответственность за правонарушения, связанные с информационной безопасностью. Назовите конкретные статьи КОАП РФ?
24. Назовите цель Федерального закона «Об информации, информационных технологиях и о защите информации»? Какие статьи регулируют отношения в сфере обеспечения информационной безопасности.
25. Назовите цель Закона «О банках и банковской деятельности» Какие статьи посвящены проблеме обеспечения ИБ
26. Назовите Цель и раскройте содержание Федерального закона «о Национальной платежной системе»
27. Какие нормативные документы существуют в сфере обеспечения информационной безопасности? Правительство РФ и ЦБ РФ
28. Что такое стандарты информационной безопасности.
29. Назовите основные функции стандартов информационной безопасности?
30. Назовите основную задачу стандартов информационной безопасности?
31. Что составляет основу стандарта ИСО 27001?
32. Опишите структуру стандарта ИСО 27001?
33. Назовите основные требования к обеспечению информационной безопасности в соответствии со стандартом СТО БР ИББС-1.0-2014. «Общие положения»;
34. Назовите основную цель и задачи стандарта Банка России «Методика оценки соответствия требованиям ИБ»;
35. О чем стандарт PCI DSS?
36. Назовите основные критерии классификации угроз безопасности операционной системы?
37. Что такое программная закладка?
38. Назовите основные модели разграничения доступа.
39. Что такое матрица доступа?
40. Какие средства защиты Windows 8 вы знаете?
41. Для чего нужны bitlocker и bitlocker to go и в чем их различия?
42. Какая система шифрования существует в ОС WINDOWS 8;
43. Для чего нужна служба управления правами в Windows 8?
44. Назовите основные составляющие службы управления правами в Windows 8.
45. Что такое брандмауэр Windows 7 и какие основные профили он предусматривает?
46. Для чего используется технология AppLocker?
47. Что такое Криптография?

48. Назовите основные функции криптографической защиты информации.
49. Основные свойства и качества алгоритма DES.
50. Основные преобразования в алгоритме AES.
51. Объясните принцип работы хэшфункции.

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

Шкала оценивания

Оценка знаний, умений, навыков проводится на основе балльно-рейтинговой системы: 30% из 100% (или 30 баллов из 100) - вклад в итоговую оценку по результатам промежуточной аттестации.

При оценивании ответа обучающегося в ходе промежуточной аттестации можно опираться на следующие критерии:

Баллы	Критерий оценки
26-30	Обучающийся показывает высокий уровень компетентности, знания программного материала, учебной, периодической и монографической литературы, законодательства и практики его применения, раскрывает не только основные понятия, но и анализирует их с точки зрения различных авторов. Обучающийся показывает не только высокий уровень теоретических знаний, но и видит междисциплинарные связи. Профессионально, грамотно, последовательно, хорошим языком четко излагает материал, аргументированно формулирует выводы. Знает в рамках требований к направлению и профилю подготовки законодательно-нормативную и практическую базу. На вопросы отвечает кратко, аргументировано, уверенно, по существу.
16-25	Обучающийся показывает достаточный уровень компетентности, знания материалов занятий, учебной и методической литературы, законодательства и практики его применения. Уверенно и профессионально, грамотным языком, ясно, четко и понятно излагает состояние и суть вопроса. Знает нормативно-законодательную и практическую базу, но при ответе допускает несущественные погрешности. Обучающийся показывает достаточный уровень профессиональных знаний, свободно оперирует понятиями, методами оценки принятия решений, имеет представление: о междисциплинарных связях, увязывает знания, полученные при изучении различных дисциплин, умеет анализировать практические ситуации, но допускает некоторые погрешности. Ответ построен логично, материал излагается хорошим языком, привлекается информативный и иллюстрированный материал, но при ответе допускает некоторые погрешности. Вопросы не вызывают существенных затруднений.
6-15	Обучающийся показывает достаточные знания материалов занятий, но при ответе отсутствует должная связь между анализом, аргументацией и выводами. На поставленные членами комиссии вопросы отвечает неуверенно, допускает погрешности. Обучающийся владеет практическими навыками, привлекает иллюстративный материал, но чувствует себя неуверенно при анализе междисциплинарных связей. В ответе не всегда присутствует логика, аргументы привлекаются недостаточно веские. На поставленные вопросы затрудняется с ответами, показывает недостаточно глубокие знания.
0-5	Обучающийся показывает слабые знания материалов занятий, учебной литературы, законодательства и практики его применения, низкий уровень компетентности, неуверенное изложение вопроса. Обучающийся показывает слабый уровень профессиональных знаний, затрудняется при анализе практических си-

	туаций. Не может привести примеры из реальной практики. Неуверенно и логически непоследовательно излагает материал. Неправильно отвечает на вопросы или затрудняется с ответом.
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Шкала перевода из многобалльной системы в традиционную:

- обучающемуся выставляется оценка «не зачтено», если обучающийся набрал менее 50 баллов,
- оценка «зачтено» выставляется при условии, если обучающийся набрал от 50 до 100 баллов.

100 баллов выставляется при условии выполнения всех требований, а также при обязательном проявлении творческого отношения к предмету, умении находить оригинальные, не содержащиеся в учебниках ответы, умении работать с источниками, которые содержатся дополнительной литературе к курсу, умении соединять знания, полученные в данном курсе со знаниями других дисциплин.

4.4. Методические материалы

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций проводятся в соответствии с Уставом Академии (утв. Постановлением Правительства Российской Федерации от 12.05.2012 г. N 473), Положением о текущем контроле успеваемости обучающихся и промежуточной аттестации обучающихся в РАНХиГС (утв. Приказом ректора от 30.01.2018 г. № 02-66), Порядке организации и проведения практики обучающихся, осваивающих образовательные программы высшего образования (утв. Приказом ректора от 22.01.2018 г. №02-28).

Устный опрос является одним из основных способов проверки усвоения знаний обучающимися. Развернутый ответ студента должен представлять собой связное, логически последовательное сообщение на определенную тему, показывать его умение применять определения, правила в конкретных случаях. Основные критерии оценки устного ответа: правильность ответа по содержанию; полнота и глубина ответа; логика изложения материала (учитывается умение строить целостный, последовательный рассказ, грамотно пользоваться специальной терминологией); использование дополнительного материала.

5. Методические указания для обучающихся по освоению дисциплины

Занятия по дисциплине представлены следующими видами работ: лекциями, практическими занятиями, самостоятельной работой обучающихся.

Подготовка к занятиям должна носить систематический характер. Это позволит обучающемуся в полном объеме выполнить все требования преподавателя. Обучающимся рекомендуется изучать как основную, так и дополнительную литературу, а также знакомиться с Интернет-источниками (список приведен в рабочей программе по дисциплине).

Методические указания для обучающихся по подготовке к лекционным занятиям. Занятия лекционного вида дают систематизированные знания о наиболее сложных и актуальных проблемах изучаемой дисциплины.

Осуществляя учебные действия на лекционных занятиях, обучающиеся должны внимательно воспринимать материал, подготовленный преподавателем, мыслить, добиваться понимания изучаемого предмета. Обучающиеся должны аккуратно вести конспект. В случае недопонимания какой-либо части предмета следует в установленном порядке задать вопрос преподавателю. В процессе работы на лекции необходимо так же выполнять в конспектах модели изучаемого предмета (рисунки, схемы, чертежи и т.д.), которые использует преподаватель.

Самостоятельная подготовка обучающихся при подготовке к занятиям лекционного вида включает в себя:

– доработку конспекта лекции, которую желательно осуществлять в тот же день, пока материал еще легко воспроизводим в памяти (через 10 часов после лекции в памяти остается не более 30-40% материала). Необходимо прочитать записи, расшифровать сокращения, доработать схемы, рисунки, таблицы;

– повторение изученного на предыдущем занятии материала.

Методические указания по подготовке к опросу и тестированию. Подготовка обучающихся к опросу предполагает изучение основной/ дополнительной литературы в соответствии тематикой дисциплины.

Подготовка к тестированию требует от обучающихся тщательного изучения материала по теме или блоку тем, где акцент делается на изучение причинно-следственных связей, раскрытию природы явлений и событий, проблемных вопросов. Для подготовки необходима рабочая программа дисциплины с примерами тестов, учебно-методическим и информационным обеспечением.

Методические указания для обучающихся по выполнению контрольных работ. Контрольные работы являются одной из основных форм текущего контроля преподавателем работы обучающегося и представляет собой решение конкретной задачи. Задача должна быть решена с подробным объяснением.

Методические указания по организации самостоятельной работы обучающихся. Наряду с прослушиванием лекций и участием в обсуждении проблем на практических занятиях, учебный план предусматривает затрату обучающимися, как правило, большего числа часов для самостоятельной работы.

Эта работа складывается из изучения литературы, в том числе в связи с подготовкой к практическим занятиям, выполнения других заданий преподавателя.

Основным элементом этой работы является изучение основных разделов дисциплины, содержащейся в программе по этой дисциплине, с использованием записей лекций преподавателя, ведущего курс, и рекомендуемой программой (а в ряде случаев и дополнительно преподавателем) литературы – учебников и учебных пособий, монографий и статей по отдельным проблемам данной науки.

Приступая к изучению той или иной темы, выделяемой по предметно-систематизированному принципу, нужно по отдельности и последовательно рассмотреть каждую из частей, из которых состоит тема. При изучении курса, обучающиеся должны уметь пользоваться и научной литературой для самостоятельной подготовки к занятиям. Обучающиеся также должны научиться, используя различные научные источники, грамотно сформировать и подготовить свое научно обоснованное и логически непротиворечивое выступление на практическом занятии, анализировать конкретные факты общественной жизни, осуществлять прогноз относительно возможного направления анализа экономических процессов, формулировать и обосновывать свое мнение.

Без ясного понимания основных понятий образовательный процесс усложняется. Для повышения эффективности обучения необходимо использовать существующие терминологические справочники и толковые словари.

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. Партыка, Т.П., Попов, И.И. Информационная безопасность [Текст] / Т.П. Партыка, И.И. Попов. – М.: ФОРУМ, 2008. – 432 с.

2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие: рек. М-вом образования РФ для студентов, обучающихся по специальности "Информатика и вычислительная техника" / В.Ф. Шаньгин. – М.: Форум: ИНФРА-М, 2008. – 416 с.

3. Ярочкин, В.И. Информационная безопасность: учебник / В.И. Ярочкин. – 5-е изд. - М.: Академический Проект, 2008. – 544 с.

6.2. Дополнительная литература

1. Авдошин, С.М., Сердюк, В.А., Савельева, А.А. Технологии и продукты Microsoft в обеспечении информационной безопасности [Текст] / С.М. Авдошин, В.А. Сердюк, А.А. Савельева. – М.: ИНТУИТ, 2016. – 455 с.

2. Скрипник, Д.А. Обеспечение безопасности персональных данных [Текст] / Д.А. Скрипник. – М.: ИНТУИТ, 2011. – 122 с.

3. Талимончик, В.П. Международно-правовое регулирование отношений информационного обмена [Текст] / В.П. Талимончик. – М.: Юридический центр Пресс, 2011. – 385 с.

4. Фаронов, А.Е. Основы информационной безопасности при работе на компьютере [Текст] / А.Е. Фаронов. – ИНТУИТ, 2011. – 157 с.

5. Шаньгин, В. Ф. Информационная безопасность [Текст] / В. Ф. Шаньгин. – М.: ДМК Пресс, 2014. – 702 с.

6.3. Учебно-методическое обеспечение самостоятельной работы

1. Кузнецов И.Н. Рефераты, курсовые и дипломные работы. Методика подготовки и оформления [Электронный ресурс]: учебно-методическое пособие/ Кузнецов И.Н.— Электрон. текстовые данные.— М.: Дашков и К, 2013.— 340 с.— Режим доступа: <http://www.iprbookshop.ru/10962.html>.— ЭБС «IPRbooks».

2. Кузнецов И.Н. Рефераты, курсовые и дипломные работы. Методика подготовки и оформления [Электронный ресурс]: учебно-методическое пособие/ Кузнецов И.Н.— Электрон. текстовые данные.— М.: Дашков и К, 2016.— 340 с.— Режим доступа: <http://www.iprbookshop.ru/60500.html>.— ЭБС «IPRbooks».

3. Громкова М.Т. Педагогика высшей школы [Электронный ресурс]: учебное пособие для студентов педагогических вузов/ Громкова М.Т.— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2015.— 446 с.— Режим доступа: <http://www.iprbookshop.ru/52045.html>.— ЭБС «IPRbooks».

4. Образовательные инновации и практики карьеры: сборник методических материалов и статей. — М.: Издательский дом. «Дело» РАНХиГС, .— 192с.

6.4. Нормативные правовые документы

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» (принят Государственной Думой 8.07.2006) № 149-ФЗ// «Российская газета» от 29.07.2006, № 165.

2. Распоряжение правительства России от 24 декабря 2013 года № 2506-р о концепции развития математического образования в Российской Федерации. //»Собрание законодательства РФ, 13.01.2014, № 2 (часть I) ст. 148.

3. Об образовании в Российской Федерации: Федеральный закон от 29.12.2012 №273-ФЗ (с последующими изменениями и дополнениями).

4. Федеральный государственный образовательный стандарт 38.03.01 Экономика (уровень бакалавриата), утвержден приказом Министерством образования и науки России от 12 ноября 2015 г. № 1327 (зарегистрировано в Минюсте России 30 ноября 2015г., регистрационный номер 39906).

5. Образовательный стандарт Российской академии народного хозяйства и государственной службы при Президенте РФ (утв. приказом ректора Академии от 18 августа 2016 г. № 01-4567).

6.5. Интернет-ресурсы

Сайты журналов:

1. Information Security <http://www.itsec.ru>
2. Защита информации. Инсайд <http://www.inside-zi.ru>
3. Хакер <http://www.xakep.ru>
4. Компьютер пресс <http://www.compress.ru>
5. Мир ПК <http://www.psworld.ru>
6. Открытые системы <http://www.osp.ru>

Образовательные сайты

1. Интернет-Университет информационных технологий – ИНТУИТ.РУ
<http://www.intuit.ru>

2. Портал «Государственная служба» - <http://civilservice.ru>
3. Искусство управления информационной безопасностью <http://www.iso27000.ru>
4. Институт экономической безопасности <http://www.bre.ru/security>

Порталы

1. Информационно-коммуникационные технологии в образовании
<http://www.ict.edu.ru>
2. Информационно – правовой портал ГАРАНТ <http://www.garant.ru>
3. Совет безопасности РФ <http://www.scrf.gov.ru/>

6.6. Иные источники

1. Барабанова, М.И., Кияев, В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях [Текст]: учебное пособие / М.И. Барабанова, В.И. Кияев. – СПб, изд-во СПбГУЭФ, 2011. - 270 с.
2. Нестеров, С. Основы информационной безопасности. [Текст]: учебное пособие / С. Нестеров. – М.: Лань, 2016. – 324 с.
3. Фороузан Б.А. Криптография и безопасность сетей [Текст]: учебное пособие / Б.А. Фороузан. – М.: ИНТУИТ; БИНОМ. Лаборатория знаний, 2010.- 784 с.

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

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

Программное обеспечение: MS Office Professional Plus 2016.

Информационные справочные системы: Научная библиотека РАНХиГС. URL: <http://lib.ranepa.ru/>; Научная электронная библиотека eLibrary.ru. URL: <http://elibrary.ru/defaultx.asp>; Национальная электронная библиотека. URL: www.nns.ru; Российская государственная библиотека. URL: www.rsl.ru; Российская национальная библиотека. URL: www.nnir.ru; Электронная библиотека Grebennikon. URL: <http://grebennikon.ru/>; Электронно-библиотечная система Издательства «Лань». URL: <http://e.lanbook.com>; Электронно-библиотечная система ЮПАЙТ. URL: <http://www.biblio-online.ru/>; Электронно-библиотечная система ЭБС IPRBOOKS: <http://iprbookshop.ru/>.

Базы данных:

Bloomberg: <http://www.bloomberg.com/>

Компания "Emerging Markets Information Service" EMIS: <http://www.securities.com>

Информационный ресурс по мировой экономике компании International Monetary Fund (IMF) / Международного Валютного Фонда: <http://www.elibrary.imf.org>

Электронный ресурс Cbonds.ru: <http://cbonds.ru/>

Система профессионального анализа рынков и компаний «Спарк»: <http://www.spark-interfax.ru/>