

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

Волгоградский институт управления - филиал РАНХиГС
Экономический факультет
Кафедра информационных систем и математического моделирования

УТВЕРЖДЕНА
учёным советом
Волгоградского института управления –
филиала РАНХиГС
Протокол № 2 от 23.09.2021 г.

АДАптированная программа специалитета

"Экономико-правовое обеспечение экономической безопасности"

(наименование образовательной программы)

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ,
реализуемой без применения электронного (онлайн) курса
для обучающихся с ограниченными возможностями здоровья и обучающихся
инвалидов**

**Б1.В.ДВ.09.02 Основы информационной безопасности
хозяйственной деятельности**

(код и наименование дисциплины)

38.05.01 Экономическая безопасность

(код, наименование направления подготовки /специальности)

Очная, заочная

(форма (формы) обучения)

Год набора – 2022 г.

Волгоград, 2021 г.

Автор-составитель:

Кандидат технических наук, доцент кафедры
информационных систем и математического моделирования

И.П. Михнев

(ученая степень и(или) ученое звание, должность) (наименование кафедры) (Ф.И.О.)

Заведующий кафедрой
информационных систем и математического моделирования, к.т.н., доцент О.А. Астафурова

(наименование кафедры) (ученая степень и(или) ученое звание) (Ф.И.О.)

РПД Б1.В.ДВ.09.02 «Основы информационной безопасности хозяйственной деятельности»
одобрена на заседании кафедры информационных систем и математического моделирования.
Протокол от «31» августа 2021 г. № 1

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы	4
1.1. Осваиваемые компетенции	4
1.2. Результаты обучения	4
2. Объем и место дисциплины в структуре ОП ВО	5
3. Содержание и структура дисциплины	5
3.1. Структура дисциплины	5
3.2. Содержание дисциплины	6
4. Материалы текущего контроля успеваемости обучающихся	12
4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации	12
4.2. Типовые материалы текущего контроля успеваемости обучающихся	13
5. Оценочные материалы промежуточной аттестации по дисциплине	22
5.1. Методы проведения зачета	22
5.2. Оценочные материалы промежуточной аттестации	22
6. Методические материалы по освоению дисциплины	34
7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет	41
7.1. Основная литература	41
7.2. Дополнительная литература	41
7.3. Нормативные правовые документы и иная правовая информация	41
7.4. Интернет-ресурсы, справочные системы	42
7.5. Иные источники	42
8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы	42

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

1.1. Осваиваемые компетенции

Дисциплина **Б1.В.ДВ.09.02 Основы информационной безопасности хозяйственной деятельности** обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПКо2 ОС-3	Способность принимать оптимальные управленческие решения с учетом критериев социально-экономической эффективности, рисков и возможностей использования имеющихся ресурсов	ПКо2 ОС-3.1	Способность использовать программные продукты для формирования и анализа баз данных и правовой информации с целью обеспечения информационной безопасности

1.2. Результаты обучения

В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ (при наличии профстандарта) трудовые или профессиональные действия	Код этапа освоения компетенции	Результаты обучения
ПКо2 ОС-3 направлена на формирование глубоких знаний в области информационных технологий, необходимых для приобретения навыков и умений управления информацией, как взаимосвязанной и соответствующим образом сформированной совокупности: организационных, управленческих, экономических, информационных, методических, программно-технологических аспектов деятельности по удовлетворению информационных потребностей с целью принятия эффективного решения, и по наращиванию интеллектуального потенциала в виде информационных баз данных и баз знаний.	ПКо2 ОС-3.1	на уровне знаний: – Использует международные стандарты информационного обмена; дает определение понятия угрозы, защиты, видов противников или “нарушителей”; перечисляет модели безопасности и их применение; называет методы криптографии; называет методы и способы обеспечения информационной безопасности в профессиональной деятельности; идентифицирует информационные технологии в системе мер защиты информации; применяет нормативные документы по защите информации и организации соответствующих отделов в организациях; применяет руководящие документы, касающиеся государственной тайны.
		на уровне умений: – Демонстрирует способность самообучения в современных компьютерных средах; выделяет опасности и угрозы информационной безопасности; применяет основные методы и программы защиты информации; использует методы и способы обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты служебной информации.
		на уровне навыков: – Демонстрирует навыки криптографической и стеганографической защиты информации; применяет основные методы и средства защиты информации.
ПКо2 ОС-3 направлена на составление и представление финансовой отчетности экономического субъекта/ проведение финансового анализа, применение знания в современных компьютерных средах и выделения опасности угроз информационной безопасности. (Проф. стандарт «Бухгалтер», утв. Приказом Минтруда России от 22	ПКо2 ОС-3.2	на уровне знаний: – Демонстрирует знания основных методов криптографии, моделей безопасности, понятия угрозы, защиты и способов обеспечения информационной безопасности в профессиональной деятельности
		на уровне умений: – Применяет знания в современных компьютерных средах и выделяет опасности угроз информационной безопасности. Применяет основные методы и программы защиты информации

декабря 2014 г. N 1061н)		на уровне навыков: – Свободно владеет навыками криптографической и стенографической защиты информации, основными методами и средствами защиты информации
--------------------------	--	---

Заполняются только те результаты обучения, которые планируется сформировать в рамках дисциплины (модуля). Отдельные уровни, не формируемые в дисциплине (модуле), могут не указываться.

2. Объем и место дисциплины в структуре ОП ВО

Учебная дисциплина **Б1.В.ДВ.09.02 «Основы информационной безопасности хозяйственной деятельности»** относится к дисциплинам по выбору вариативной части учебного плана (часть, формируемая участниками образовательных отношений). Дисциплина общим объемом 108 час изучается в течение одного семестра. На очной форме обучения дисциплина изучается в 4 семестре. Общая трудоемкость дисциплины в зачетных единицах составляет 3 ЗЕ (108 час).

Для успешного овладения дисциплиной студенту необходимо использовать знания и навыки, полученные им при изучении таких дисциплин, как математика, физика, Б1.В.ДВ.1.2 Логика, Б1.Б.6.1 Математика, Б1.Б.9 Экономическая теория, Б1.Б.36 Национальная безопасность.

Знания, полученные в ходе изучения дисциплины «Основы информационной безопасности хозяйственной деятельности» могут быть полезны при изучении таких профессиональных дисциплин, как Б1.Б.21 «Бухгалтерский учет и анализ», Б1.Б.30 «Основы финансовых вычислений».

По очной форме обучения количество академических часов, выделенных на контактную работу с преподавателем (по видам учебных занятий) – 52 час и на самостоятельную работу обучающихся – 56 часов. В соответствии с учебным планом формой промежуточной аттестации является зачет с оценкой.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.				СРО	Форма текущего контроля успеваемости ⁴ , промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				
			Л/ЭО, ДОТ*	ЛР/ЭО, ДОТ*	ПЗ/ЭО, ДОТ*		
Очная форма обучения							
<i>4 семестр</i>							
Тема 1	Понятие информации, защиты информации и информационной безопасности. Основные составляющие.	12	2	-	4	6	О
Тема 2	Законодательный уровень информационной безопасности. Компьютерные преступления. Ответственность за совершение компьютерных преступлений.	12	2	-	4	6	О
Тема 3	Классификация атак. Понятие угрозы. Модель угроз. Рекомендации по обеспечению информационной безопасности.	12	2	-	4	6	О
Тема 4	Основные понятия криптографии. Два современных направления в криптографии. Классические криптосистемы.	12	2	-	4	6	О

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.					СРО	Форма текущего контроля успеваемости ⁴ , промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий					
			Л/ЭО, ДОТ*	ЛР/ЭО, ДОТ*	ПЗ/ЭО, ДОТ*	КСР		
Тема 5	Криптография с открытым ключом. Системы шифрования, не требующие передачи ключа. Электронная подпись.	16	4	-	4		8	О
Тема 6	Основные технологии построения защищенных ИС. Межсетевые экраны.	12	2	-	4		6	О
Тема 7	Технология VPN-сетей.	12	2	-	4		6	О
Тема 8	Защита информации в Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей.	10	2	-	2		6	О
Тема 9	Типовая структура защиты от НСД. Управление доступом.	10	2	-	2		6	О, Т
Промежуточная аттестация								Зач. с оценкой
Всего:		108	20		32		56	3 ЗЕ

Примечание: 4 – формы текущего контроля успеваемости: опрос (О), тестирование (Т), контрольная работа (КР), коллоквиум (К), эссе (Э), реферат (Р), диспут (Д), задания (З) и др.

Самостоятельная работа (СР) по изучению дисциплины осуществляется с применением ДОТ. Доступ к ДОТ осуществляется каждым обучающимся самостоятельно с любого устройства на портале: <https://lms.ganepa.ru>. Пароль и логин к личному кабинету/профилю/учетной записи предоставляется обучающемуся деканатом.

3.2 Содержание дисциплины (модуля)

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)
Тема 1	Понятие информации, защиты информации и информационной безопасности. Основные составляющие.	Понятие информации, защиты информации и информационной безопасности. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства, на уровне региона и на локальном уровне. Основные положения теории информационной безопасности информационных систем. Основные составляющие обеспечения информационной безопасности хозяйственной деятельности.

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)
Тема 2	Законодательный уровень информационной безопасности. Компьютерные преступления. Ответственность за совершение компьютерных преступлений.	<p>Важность законодательного уровня информационной безопасности. Обзор российского законодательства в области обеспечения информационной безопасности. Доктрина информационной безопасности РФ, законы «О государственной тайне», «Об информации, информационных технологиях и о защите информации». Другие законы и законодательные акты. Концепция информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны и конфиденциальной информации, нормативно-справочные документы. Нормативные акты администрации Волгограда в области информационной безопасности.</p> <p>Компьютерные преступления. Ответственность за совершение компьютерных преступлений. Уголовная и административная ответственность.</p>
Тема 3	Классификация атак. Понятие угрозы. Модель угроз. Рекомендации по обеспечению информационной безопасности.	<p>Понятие атаки на информационную систему. Классификация атак. Виды противников или “нарушителей”, их классификация. Каналы утечки информации: визуально-оптический, акустический, электромагнитный и материально-вещественный. Понятие угрозы. Источники угроз и их классификация. Построение модели угроз организации. Примеры. Руководящие документы Гостехкомиссии России (Федеральная служба по техническому и экспортному контролю) по защите от несанкционированного доступа к информации. Специальные требования и рекомендации. Инструкция СТР-К. Рекомендации по защите конфиденциальной информации. Классы защищенности средств вычислительной техники и автоматизированных систем по руководящим документам Гостехкомиссии России. Показатели защищенности. Система защиты информации от несанкционированного доступа. Рекомендуемые меры по обеспечению защиты информации в процессе эксплуатации информационной системы. Разрешительная система допуска. Рекомендации по плану доработки объектов информатизации на соответствие требованиям руководящих документов Гостехкомиссии России.</p>

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)
Тема 4	Основные понятия криптографии. Два современных направления в криптографии. Классические криптосистемы.	Историческая справка. Возможные направления решения задачи обеспечения передачи секретной информации. Стеганография и криптография. Важность криптографии при решении задач обеспечения информационной безопасности хозяйственной деятельности и сохранения конфиденциальной информации. Основные понятия криптографии. Понятие криптосистемы, ключа. Возможные атаки на криптосистемы, понятие криптоанализа. Надежность криптосистемы. Два основных направления в современной криптографии. Классические криптосистемы. Одноалфавитные и многоалфавитные криптосистемы. Системы Цезаря и Виженера. Возможности криптоанализа многоалфавитных систем. Раскрытие системы Виженера. Надежность многоалфавитных систем. Электромеханические шифровальные машины. Абсолютно надежная криптосистема: “Одноразовый блокнот”. Возможность использования таких систем на практике. Стандарты шифрования данных. Криптосистема DES. Российский стандарт шифрования ГОСТ 28147-89. Проблема выбора надежной криптосистемы для защиты своих данных. Перспективы развития криптоанализа. Проблема полного перебора всех ключей.
Тема 5	Криптография с открытым ключом. Системы шифрования, не требующие передачи ключа. Электронная подпись.	Системы шифрования, не требующие передачи ключа. Проблемы использования таких систем. Протокол использования системы «Одноразовый блокнот», не требующий первоначального обмена секретными ключами. Криптография с открытым ключом. Понятие открытого и секретного ключа. Правила их использования. Принципы построения криптосистем с открытым ключом. Известные криптосистемы с открытым ключом и их алгоритмы. Система RSA. Длина ключа в криптографии с открытым ключом. Односторонняя функция, возможность ее использования. Электронная подпись и принципы ее применения.
Тема 6	Основные технологии построения защищенных ИС. Межсетевые экраны.	Основные технологии построения защищенных ИС. Понятие меж сетевого экрана. Правила фильтрации и принципы их применения. Пакетные фильтры. Политика сетевой безопасности. Политика реализации межсетевых экранов. Функциональные требования к межсетевым экранам и их компоненты. Шлюзы сеансового и прикладного уровня. Новые функции брандмауэров. Схемы организации межсетевых экранов. Особенности различных схем реализации, их преимущества и недостатки. Проблемы, связанные с межсетевыми экранами. Требования к межсетевым экранам

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)
Тема 7	Технология VPN-сетей.	Технология объединения локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи данных в единую виртуальную сеть, обеспечивающую защиту информационных потоков или технология VPN-сетей. Особенности VPN. Туннель VPN. Туннелирование и его особенности. Основные разновидности VPN-устройств по технической реализации. Роли VPN-устройств. Варианты построения защищенных каналов VPN. Угрозы для VPN. Варианты защищенных соединений. Классификация VPN-сетей. Совмещение VPN-технологий и межсетевых экранов. Недостатки VPN.
Тема 8	Защита информации в Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей.	Проблема обеспечения информационной безопасности при работе с глобальной сетью Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей. Указ президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена». Угрозы информационной безопасности при работе с Интернет. Вирусы, исполняемые модули, всплывающие окна и реклама. Использование антивирусных программ и межсетевых экранов при работе с Интернет. Программные средства проверки трафика и борьбы с несанкционированным использованием ресурсов информационной системы.
Тема 9	Типовая структура защиты от НСД. Управление доступом.	Архитектура типовой системы защиты от несанкционированного доступа. Идентификация и аутентификация. Парольная аутентификация. Правила применения паролей. Одноразовые пароли. Сервер аутентификации. Подсистема управления доступом, подсистема регистрации и учета. Принципы контроля доступа. Матрица доступа и списки доступа. Произвольное и принудительное управление доступом. Ограничивающий интерфейс. Ролевое управление доступом. Статическое и динамическое распределение ролей. Подсистема обеспечения целостности. Криптографическая подсистема. Программно-аппаратные средства защиты информации от НСД. Устройства ввода идентификационных признаков. Классификация устройств ввода идентификационных признаков. Биометрические устройства ввода идентификационных признаков и их классификация. Преимущества и недостатки их использования. Комбинированные устройства. Электронные замки.

На самостоятельную работу студентов по дисциплине **Б1.В.ДВ.09.02 Основы информационной безопасности хозяйственной деятельности** выносятся следующие темы:

№ п/п	Тема	Вопросы, выносимые на СРС	Очная форма	Заочная форма
1	2	3	4	5
1.	Понятие информации, защиты информации и информации и	Понятие информации, защиты информации и информационной безопасности. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства, на уровне	0	0

	информационн ой безопасности. Основные составляющие.	региона и на локальном уровне. Основные положения теории информационной безопасности информационных систем.		
2.	Законодательн ый уровень информационн ой безопасности. Компьютерные преступления. Ответственнос ть за совершение компьютерных преступлений.	Обзор российского законодательства в области обеспечения информационной безопасности. Доктрина информационной безопасности РФ, законы «О государственной тайне», «Об информации, информационных технологиях и о защите информации». Основные нормативные руководящие документы, касающиеся государственной тайны и конфиденциальной информации. Нормативные акты администрации Волгограда в области информационной безопасности.	<i>o</i>	<i>o</i>
3.	Классификаци я атак. Понятие угрозы. Модель угроз. Рекомендации по обеспечению информационн ой безопасности.	Понятие атаки на информационную систему. Классификация атак. Виды противников или “нарушителей”, их классификация. Каналы утечки информации: визуально-оптический, акустический, электромагнитный и материально- вещественный. Понятие угрозы. Источники угроз и их классификация. Построение модели угроз организации. Примеры. Специальные требования и рекомендации. Показатели защищенности. Система защиты информации от несанкционированного доступа. Рекомендуемые меры по обеспечению защиты информации в процессе эксплуатации информационной системы. Разрешительная система допуска.	<i>o</i>	<i>o</i>
4.	Основные понятия криптографии. Два современных направления в криптографии. Классические криптосистем ы.	Стеганография и криптография. Важность криптографии при решении задач обеспечения информационной безопасности хозяйственной деятельности и сохранения конфиденциальной информации. Основные понятия криптографии. Понятие криптосистемы, ключа. Возможные атаки на криптосистемы, понятие криптоанализа. Надежность криптосистемы. Два основных направления в современной криптографии. Одноалфавитные и многоалфавитные криптосистемы. Системы Цезаря и Виженера. Возможности криптоанализа многоалфавитных систем. Раскрытие системы Виженера. Надежность многоалфавитных систем. Абсолютно надежная криптосистема: “Одноразовый блокнот”. Криптосистема DES.	<i>o</i>	<i>o</i>
5	Криптография с открытым ключом. Системы шифрования, не требующие передачи	Системы шифрования, не требующие передачи ключа. Протокол использования системы «Одноразовый блокнот», не требующий первоначального обмена секретными ключами. Криптография с открытым ключом. Понятие открытого и секретного ключа. Принципы построения криптосистем с открытым ключом.	<i>o</i>	<i>o</i>

	ключа. Электронная подпись.	Известные криптосистемы с открытым ключом и их алгоритмы. Система RSA. Длина ключа в криптографии с открытым ключом. Односторонняя функция, возможность ее использования. Электронная подпись и принципы ее применения.		
6	Основные технологии построения защищенных ИС. Межсетевые экраны.	Основные технологии построения защищенных ИС. Понятие меж сетевого экрана. Правила фильтрации и принципы их применения. Пакетные фильтры. Политика сетевой безопасности. Политика реализации межсетевых экранов. Функциональные требования к межсетевым экранам и их компоненты. Шлюзы сеансового и прикладного уровня. Новые функции брандмауэров. Схемы организации межсетевых экранов. Требования к межсетевым экранам	0	0
7	Технология VPN-сетей.	Технология объединения локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи данных в единую виртуальную сеть, обеспечивающую защиту информационных потоков или технология VPN-сетей. Особенности VPN. Туннелирование и его особенности. Основные разновидности VPN-устройств по технической реализации. Роли VPN-устройств. Варианты построения защищенных каналов VPN. Угрозы для VPN. Классификация VPN-сетей. Совмещение VPN-технологий и меж сетевого экрана. Недостатки VPN.	0	0
8	Защита информации в Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей.	Проблема обеспечения информационной безопасности при работе с глобальной сетью Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей. Указ президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена». Угрозы информационной безопасности при работе с Интернет. Вирусы, исполняемые модули, всплывающие окна и реклама. Использование антивирусных программ и межсетевых экранов при работе с Интернет. Программные средства проверки трафика и борьбы с несанкционированным использованием ресурсов информационной системы.	0	0

9	Типовая структура защиты от НСД. Управление доступом.	Архитектура типовой системы защиты от несанкционированного доступа. Идентификация и аутентификация. Парольная аутентификация. Правила применения паролей. Одноразовые пароли. Принципы контроля доступа. Матрица доступа и списки доступа. Произвольное и принудительное управление доступом. Ограничивающий интерфейс. Ролевое управление доступом. Криптографическая подсистема. Программно-аппаратные средства защиты информации от НСД. Устройства ввода идентифицируемых признаков. Преимущества и недостатки их использования. Электронные замки.	O, T	O, T
---	---	---	------	------

4. Материалы текущего контроля успеваемости обучающихся

4.1. Формы и методы текущего контроля успеваемости и промежуточной аттестации

В ходе реализации дисциплины **Б1.В.ДВ.09.02 «Основы информационной безопасности хозяйственной деятельности»** используются следующие методы текущего контроля успеваемости обучающихся:

№ п/п	Наименование тем (разделов)	Методы текущего контроля успеваемости
Очная форма		
Тема 1	Понятие информации, защиты информации и информационной безопасности. Основные составляющие.	Устный опрос
Тема 2	Законодательный уровень информационной безопасности. Компьютерные преступления. Ответственность за совершение компьютерных преступлений.	Устный опрос
Тема 3	Классификация атак. Понятие угрозы. Модель угроз. Рекомендации по обеспечению информационной безопасности.	Устный опрос
Тема 4	Основные понятия криптографии. Два современных направления в криптографии. Классические криптосистемы.	Устный опрос
Тема 5	Криптография с открытым ключом. Системы шифрования, не требующие передачи ключа. Электронная подпись.	Устный опрос
Тема 6	Основные технологии построения защищенных ИС. Межсетевые экраны.	Устный опрос
Тема 7	Технология VPN-сетей.	Устный опрос
Тема 8	Защита информации в Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей.	Устный опрос
Тема 9	Типовая структура защиты от НСД. Управление доступом.	Устный опрос, тестирование

При проведении занятий лекционного типа: устный опрос;
при проведении занятий семинарского типа: индивидуальные задания для выполнения на компьютере;
при контроле результатов самостоятельной работы студентов: электронные тесты.

Промежуточная аттестация проводится в форме зачета методом электронного тестирования. К сдаче зачета по дисциплине допускаются студенты, получившие не меньше 60 баллов при текущей аттестации. При подготовке к зачету студент внимательно просматривает вопросы, предусмотренные рабочей программой, и знакомится с рекомендованной основной литературой. Основой для сдачи зачета студентом является изучение конспектов обзорных лекций, прослушанных в течение семестра, информация, полученная в результате самостоятельной работы, и практические навыки, освоенные при решении задач в течение семестра.

4.2. Типовые материалы текущего контроля успеваемости обучающихся

Задания для контактной и самостоятельной работы включают в себя комплекс заданий выполнение, которых, предполагает тщательное изучение научной и учебной литературы, периодических изданий, а также законодательных и нормативных документов, предлагаемых в п.6 «Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет, учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине».

Задания предоставляются на проверку в электронном виде или на бумажном носителе. Предложенные задания выполняются в форме устного опроса, мультимедийного доклада, решения задач на компьютере, электронного теста и т.п.

Тема 1

Понятие информации, защиты информации и информационной безопасности.

Основные составляющие.

Вопросы устного опроса:

1. Понятие информации, защиты информации и информационной безопасности.
2. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства, на уровне региона и на локальном уровне.
3. Основные положения теории информационной безопасности информационных систем.
4. Основные составляющие обеспечения информационной безопасности хозяйственной деятельности.

Тема 2

Законодательный уровень информационной безопасности. Компьютерные преступления. Ответственность за совершение компьютерных преступлений.

Вопросы устного опроса:

1. Важность законодательного уровня информационной безопасности.
2. Обзор российского законодательства в области обеспечения информационной безопасности.
3. Доктрина информационной безопасности РФ, законы «О государственной тайне», «Об информации, информационных технологиях и о защите информации».
4. Другие законы и законодательные акты. Концепция информационной безопасности.
5. Основные нормативные руководящие документы, касающиеся государственной тайны и конфиденциальной информации, нормативно-справочные документы. Нормативные акты администрации Волгограда в области информационной безопасности.
6. Компьютерные преступления. Ответственность за совершение компьютерных преступлений.
7. Уголовная и административная ответственность.

Тема 3

Классификация атак. Понятие угрозы. Модель угроз. Рекомендации по обеспечению информационной безопасности.

Вопросы устного опроса:

1. Понятие атаки на информационную систему.
2. Классификация атак. Виды противников или “нарушителей”, их классификация.
3. Каналы утечки информации: визуально-оптический, акустический, электромагнитный и материально-вещественный.
4. Понятие угрозы. Источники угроз и их классификация.

5. Построение модели угроз организации. Примеры.
6. Руководящие документы Гостехкомиссии России (Федеральная служба по техническому и экспортному контролю) по защите от несанкционированного доступа к информации. Специальные требования и рекомендации. Инструкция СТР-К.
7. Рекомендации по защите конфиденциальной информации. Классы защищенности средств вычислительной техники и автоматизированных систем по руководящим документам Гостехкомиссии России.
8. Показатели защищенности. Система защиты информации от несанкционированного доступа.
9. Рекомендуемые меры по обеспечению защиты информации в процессе эксплуатации информационной системы.
10. Разрешительная система допуска. Рекомендации по плану доработки объектов информатизации на соответствие требованиям руководящих документов Гостехкомиссии России.

Тема 4

Основные понятия криптографии. Два современных направления в криптографии.

Классические криптосистемы.

Вопросы устного опроса:

1. Историческая справка. Возможные направления решения задачи обеспечения передачи секретной информации.
2. Стеганография и криптография. Важность криптографии при решении задач обеспечения информационной безопасности хозяйственной деятельности и сохранения конфиденциальной информации.
3. Основные понятия криптографии. Понятие криптосистемы, ключа. Возможные атаки на криптосистемы, понятие криптоанализа.
4. Надежность криптосистемы. Два основных направления в современной криптографии. Классические криптосистемы.
5. Одноалфавитные и многоалфавитные криптосистемы.
6. Системы Цезаря и Виженера. Возможности криптоанализа многоалфавитных систем. Раскрытие системы Виженера.
7. Надежность многоалфавитных систем. Электромеханические шифровальные машины.
8. Абсолютно надежная криптосистема: «Одноразовый блокнот». Возможность использования таких систем на практике. Стандарты шифрования данных.
9. Криптосистема DES. Российский стандарт шифрования ГОСТ 28147-89. Проблема выбора надежной криптосистемы для защиты своих данных.
10. Перспективы развития криптоанализа. Проблема полного перебора всех ключей.

Тема 5

Криптография с открытым ключом. Системы шифрования, не требующие передачи ключа. Электронная подпись.

Вопросы устного опроса:

1. Системы шифрования, не требующие передачи ключа.
2. Проблемы использования таких систем. Протокол использования системы «Одноразовый блокнот», не требующий первоначального обмена секретными ключами. Криптография с открытым ключом.
3. Понятие открытого и секретного ключа. Правила их использования.
4. Принципы построения криптосистем с открытым ключом.
5. Известные криптосистемы с открытым ключом и их алгоритмы. Система RSA.
6. Длина ключа в криптографии с открытым ключом.
7. Односторонняя функция, возможность ее использования.
8. Электронная подпись и принципы ее применения.

Тема 6

Основные технологии построения защищенных ИС. Межсетевые экраны.

Вопросы устного опроса:

1. Основные технологии построения защищенных ИС.
2. Понятие межсетевого экрана. Правила фильтрации и принципы их применения. Пакетные

- фильтры. Политика сетевой безопасности.
3. Политика реализации межсетевых экранов. Функциональные требования к межсетевым экранам и их компоненты.
 4. Шлюзы сеансового и прикладного уровня. Новые функции брандмауэров.
 5. Схемы организации межсетевых экранов. Особенности различных схем реализации, их преимущества и недостатки.
 6. Проблемы, связанные с межсетевыми экранами.
 7. Требования к межсетевым экранам

Тема 7

Технология VPN-сетей.

Вопросы устного опроса:

1. Технология объединения локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи данных в единую виртуальную сеть, обеспечивающую защиту информационных потоков или технология VPN-сетей.
2. Особенности VPN. Туннель VPN. Туннелирование и его особенности.
3. Основные разновидности VPN-устройств по технической реализации. Роли VPN-устройств. Варианты построения защищенных каналов VPN.
4. Угрозы для VPN. Варианты защищенных соединений.
5. Классификация VPN-сетей. Совмещение VPN-технологий и межсетевого экрана. Недостатки VPN.

Тема 8

Защита информации в Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей.

Вопросы устного опроса:

1. Проблема обеспечения информационной безопасности при работе с глобальной сетью Интернет.
2. Информационная безопасность в условиях функционирования в России глобальных сетей.
3. Указ президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена». Угрозы информационной безопасности при работе с Интернет.
4. Вирусы, исполняемые модули, всплывающие окна и реклама. Использование антивирусных программ и межсетевых экранов при работе с Интернет.
5. Программные средства проверки трафика и борьбы с несанкционированным использованием ресурсов информационной системы.

Тема 9

Типовая структура защиты от НСД. Управление доступом.

Вопросы устного опроса:

1. Архитектура типовой системы защиты от несанкционированного доступа. Идентификация и аутентификация.
2. Парольная аутентификация. Правила применения паролей.
3. Одноразовые пароли. Сервер аутентификации. Подсистема управления доступом, подсистема регистрации и учета.
4. Принципы контроля доступа. Матрица доступа и списки доступа.
5. Произвольное и принудительное управление доступом. Ограничивающий интерфейс.
6. Ролевое управление доступом. Статическое и динамическое распределение ролей. Подсистема обеспечения целостности. Криптографическая подсистема.
7. Программно-аппаратные средства защиты информации от НСД. Устройства ввода идентификационных признаков. Классификация устройств ввода идентификационных признаков. Биометрические устройства ввода идентификационных признаков и их классификация.
8. Преимущества и недостатки их использования. Комбинированные устройства. Электронные замки.

ИТОГОВЫЙ ТЕСТ ПО КУРСУ
«Основы информационной безопасности хозяйственной деятельности»

Электронный тест представляет собой задания с выбором только одного правильного ответа из предложенных. Результат программа Unitest выводит в процентах.

1. Криптография это

- A) наука о методах преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для несанкционированных лиц
- B) наука о методах и способах раскрытия шифров
- C) совокупность методов, скрывающих факт передачи секретной информации за открытой информацией
- D) совокупность методов, обеспечивающих абсолютную надежность канала передачи данных от перехвата
- E) наука о методах создания цифровой подписи

2. Какая из следующих криптоаналитических атак считается наиболее опасной?

- A) при наличии только одного зашифрованного фрагмента
- B) при наличии большого набора зашифрованных фрагментов
- C) при наличии фрагмента открытого текста и соответствующего ему криптотекста
- D) при известном методе шифрования
- E) при возможности выбора любого открытого текста и получении соответствующего ему криптотекста

3. Сколько различных ключей в системе Цезаря при использовании полного русского алфавита?

- A) 16
- B) 33
- C) 66
- D) 256
- E) 1024

4. Что является ключом в криптосистеме Виженера?

- A) любое дробное число
- B) величина сдвига исходного алфавита
- C) переставленный алфавит
- D) случайная последовательность букв, равная длине сообщения
- E) любое слово

5. Какая из перечисленных криптосистем является системой с открытым ключом?

- A) DES
- B) RSA
- C) Энигма
- D) ГОСТ 28147
- E) Цезаря

6. Можно ли в программе PGP воспользоваться чужим открытым ключом для расшифрования информации.

- A) да
- B) нет
- C) да, если известен тот пароль
- D) да, если пользователь даст права на расшифровку его информации и сообщит свой пароль
- E) да, если перебрать все ключи

7. Как раскрываются криптосистемы одноалфавитной замены?

- A) такие системы раскрыть нельзя
- B) полный перебор ключей
- C) анализ частот встречаемых букв

- D) перебор сообщений
- E) перестановки букв криптотекста

8. Криптоанализ это

- A) наука о методах преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для несанкционированных лиц
- B) наука о методах и способах раскрытия шифров
- C) совокупность методов, скрывающих факт передачи секретной информации за открытой информацией
- D) совокупность методов, обеспечивающих абсолютную надежность канала передачи данных от перехвата
- E) наука о методах создания цифровой подписи

9. Что является ключом в криптосистеме Цезаря?

- A) любое слово
- B) любое число
- C) величина сдвига исходного алфавита
- D) переставленный алфавит
- E) случайная последовательность символов

10. Какова длина ключа в стандарте шифрования ГОСТ 28147?

- A) 256 бит
- B) 64 бит
- C) 56 бит
- D) 1024 бит
- E) 2048 бит

11. На сложности решения какой математической задачи основана система RSA?

- A) коды исправляющие ошибки
- B) дискретный логарифм
- C) задача “о рюкзаке”
- D) разложение больших чисел на простые множители
- E) сложение по модулю два

12. Криптографический протокол это

- A) метод шифрования данных
- B) метод криптоанализа данных
- C) метод перехвата данных
- D) алгоритм обмена информацией между различными участниками при секретной передаче данных
- E) особая криптосистема

13. Криптосистема «Одноразовый блокнот» это:

- A) перестановочная система
- B) одноалфавитная система простой замены
- C) многоалфавитная система
- D) система с открытым ключом
- E) такой системы не существует

14. Какой пароль наиболее надежен?

- A) Фамилия пользователя
- B) Фраза из книги
- C) случайная последовательность цифр
- D) случайная последовательность букв
- E) случайная последовательность произвольных символов

15. Какова длина ключа в системе шифрования DES?

- A) 256 бит
- B) 64 бит
- C) 2048 бит
- D) 1024 бит
- E) 512 бит

16. Криптотекст это

- A) текст исходного сообщения
- B) текст зашифрованного сообщения
- C) пароль
- D) текст, полученный при криптоанализе
- E) ключ

17. Тайнопись (стеганография) это

- A) наука о методах преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для несанкционированных лиц
- B) наука о методах и способах раскрытия шифров
- C) совокупность методов, скрывающих факт передачи секретной информации за открытой информацией
- D) совокупность методов, обеспечивающих абсолютную надежность канала передачи данных от перехвата
- E) наука о методах создания цифровой подписи

18. Что позволяет определить метод Казиски при криптоанализе системы Виженера?

- A) пароль
- B) открытый текст
- C) метод шифрования
- D) длину пароля
- E) длину открытого текста

19. Какая криптосистема обеспечивает абсолютную надежность защиты при правильном ее использовании?

- A) DES
- B) RSA
- C) ГОСТ 28147
- D) Одноразовый блокнот
- E) Виженера

20. Обеспечивает ли пароль на вход в Windows надежную защиту компьютера?

- A) да
- B) нет
- C) при длине пароля более 10 символов
- D) при случайном пароле
- E) при регулярной смене пароля

21. Можно ли в программе PGP воспользоваться чужим открытым ключом для расшифровки информации.

- A) да
- B) нет
- C) да, если известен тот пароль
- D) да, если пользователь даст права на расшифровку его информации и сообщит свой пароль
- E) да, если перебрать все ключи

22. Как раскрываются криптосистемы одноалфавитной замены?

- A) такие системы раскрыть нельзя
- B) полный перебор ключей
- C) анализ частот встречаемых букв

- D) перебор сообщений
- E) перестановки букв криптотекста

23. Криптоанализ это

- A) наука о методах преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для несанкционированных лиц
- B) наука о методах и способах раскрытия шифров
- C) совокупность методов, скрывающих факт передачи секретной информации за открытой информацией
- D) совокупность методов, обеспечивающих абсолютную надежность канала передачи данных от перехвата
- E) наука о методах создания цифровой подписи

24. Что является ключом в криптосистеме Цезаря?

- A) любое слово
- B) любое число
- C) величина сдвига исходного алфавита
- D) переставленный алфавит
- E) случайная последовательность символов

25. Какова длина ключа в стандарте шифрования ГОСТ 28147?

- A) 256 бит
- B) 64 бит
- C) 56 бит
- D) 1024 бит
- E) 2048 бит

26. На сложности решения какой математической задачи основана система RSA?

- A) коды исправляющие ошибки
- B) дискретный логарифм
- C) задача “о рюкзаке”
- D) разложение больших чисел на простые множители
- E) сложение по модулю два

27. Криптографический протокол это

- A) метод шифрования данных
- B) метод криптоанализа данных
- C) метод перехвата данных
- D) алгоритм обмена информацией между различными участниками при секретной передаче данных
- E) особая криптосистема

27. Криптосистема «Одноразовый блокнот» это:

- A) перестановочная система
- B) одноалфавитная система простой замены
- C) многоалфавитная система
- D) система с открытым ключом
- E) такой системы не существует

29. Какой пароль наиболее надежен?

- A) Фамилия пользователя
- B) Фраза из книги
- C) случайная последовательность цифр
- D) случайная последовательность букв
- E) случайная последовательность произвольных символов

30. Какова длина ключа в системе шифрования DES?

- A) 256 бит D) 1024 бит
B) 64 бит E) 512 бит
C) 2048 бит

Шкала оценивания Устный опрос

Уровень знаний, умений и навыков обучающегося при устном ответе во время текущего контроля определяется оценками «Отлично»/ «Хорошо»/ «Удовлетворительно»/ «Неудовлетворительно».

В Волгоградском институте управления – филиале РАНХиГС принята следующая шкала соответствия рейтинговых оценок пятибалльным оценкам:

- 90 – 100% – «отлично» (5);
- 75 – 89% – «хорошо» (4);
- 60 – 74 – «удовлетворительно» (3);
- менее 60% – «неудовлетворительно» (2).

Уровень знаний, умений и навыков обучающегося при устном ответе во время проведения текущего контроля определяется баллами в диапазоне 0-100 %. Критериями оценивания при проведении устного опроса является демонстрация основных теоретических положений, в рамках осваиваемой компетенции, умение применять полученные знания на практике, овладение навыками анализа и систематизации информации.

При оценивании результатов устного опроса используется следующая шкала оценок:

100% - 90% (отлично)	Этапы компетенции, предусмотренные образовательной программой, сформированы на высоком уровне. Свободное владение материалом, выявление межпредметных связей. Уверенное владение понятийным аппаратом дисциплины. Практические навыки профессиональной деятельности сформированы на высоком уровне. Способность к самостоятельному нестандартному решению практических задач
89% - 75% (хорошо)	Этапы компетенции, предусмотренные образовательной программой, сформированы достаточно. Детальное воспроизведение учебного материала. Практические навыки профессиональной деятельности в значительной мере сформированы. Присутствуют навыки самостоятельного решения практических задач с отдельными элементами творчества.
74% - 60% (удовлетворительно)	Этапы компетенции, предусмотренные образовательной программой, сформированы на минимальном уровне. Наличие минимально допустимого уровня в усвоении учебного материала, в т.ч. в самостоятельном решении практических задач. Практические навыки профессиональной деятельности сформированы не в полной мере.
менее 60% (неудовлетворительно)	Этапы компетенции, предусмотренные образовательной программой, не сформированы. Недостаточный уровень усвоения понятийного аппарата и наличие фрагментарных знаний по дисциплине. Отсутствие минимально допустимого уровня в самостоятельном решении практических задач. Практические навыки профессиональной деятельности не сформированы.

Тестирование

Уровень знаний, умений и навыков обучающегося при устном ответе во время проведения текущего контроля определяется баллами в диапазоне 0-100 %. Критерием оценивания при проведении тестирования, является количество верных ответов, которые дал

студент на вопросы теста. При расчете количества баллов, полученных студентом по итогам тестирования, используется следующая формула:

$$B = \frac{B}{O} \times 100\% ,$$

где

Б – количество баллов, полученных студентом по итогам тестирования;

В – количество верных ответов, данных студентом на вопросы теста;

О – общее количество вопросов в тесте.

Проверка реферата

Уровень знаний, умений и навыков обучающегося при проверке реферата во время проведения текущего контроля определяется баллами в диапазоне 0-100 %. Критериями оценивания при проверке реферата является демонстрация основных теоретических положений, в рамках осваиваемой компетенции.

При оценивании результатов устного опроса используется следующая шкала оценок:

100% - 90%	Учащийся демонстрирует совершенное знание основных теоретических положений, в рамках осваиваемой компетенции.
89% - 75%	Учащийся демонстрирует знание большей части основных теоретических положений, в рамках осваиваемой компетенции.
74% - 60%	Учащийся демонстрирует достаточное знание основных теоретических положений, в рамках осваиваемой компетенции.
менее 60%	Учащийся демонстрирует отсутствие знания основных теоретических положений, в рамках осваиваемой компетенции.

Проверка кейса

Уровень знаний, умений и навыков обучающегося при проверке кейса во время проведения текущего контроля определяется баллами в диапазоне 0-100 %. Критериями оценивания при проверке кейса является демонстрация основных теоретических положений, в рамках осваиваемой компетенции.

При оценивании результатов решения кейса используется следующая шкала оценок:

100% - 90%	Учащийся демонстрирует совершенное знание основных теоретических положений, практических и аналитических навыков в рамках осваиваемой компетенции.
89% - 75%	Учащийся демонстрирует знание большей части основных теоретических положений, практических и аналитических навыков в рамках осваиваемой компетенции.
74% - 60%	Учащийся демонстрирует достаточное знание основных теоретических положений, практических и аналитических навыков в рамках осваиваемой компетенции.
менее 60%	Учащийся демонстрирует отсутствие знания основных теоретических положений, практических и аналитических навыков в рамках осваиваемой компетенции.

Решение задач

Уровень знаний, умений и навыков обучающегося при решении задач во время проведения текущего контроля определяется баллами в диапазоне 0-100 %. Критерием оценивания при решении задач, является количество верно решенных задач. При расчете количества баллов, полученных студентом по итогам решения задач, используется следующая формула:

$$B = \frac{B}{O} \times 100\% ,$$

где Б – количество баллов, полученных студентом по итогам решения задач;

В – количество верно решенных задач;

О – общее количество задач.

Решение ситуационной задачи

Уровень знаний, умений и навыков обучающегося при выполнении ситуационной задачи во время проведения текущего контроля определяется баллами в диапазоне 0-100 %. Критериями оценивания является сбор и обобщение необходимой информации, правильное выполнение необходимых расчетов, достоверность и обоснованность выводов.

При оценивании результатов решения ситуационной задачи используется следующая шкала оценок:

100% - 90%	Учащийся демонстрирует совершенное знание основных теоретических положений, умеет собирать и обобщать необходимую информацию, правильно осуществляет расчеты, делает обоснованные выводы
89% - 75%	Учащийся демонстрирует знание большей части основных теоретических положений, может собрать большую часть необходимой информации, рассчитывает необходимые показатели, делает выводы, допуская при этом незначительные ошибки
74% - 60%	Учащийся демонстрирует знание некоторой части основных теоретических положений, может собрать некоторую часть необходимой информации, рассчитывает необходимые показатели, делает выводы, допуская при этом ошибки
менее 60%	Учащийся демонстрирует отсутствие знания основных теоретических положений, умений и навыков в рамках осваиваемой компетенции.

5. Оценочные материалы промежуточной аттестации по дисциплине

5.1. Методы проведения зачета с оценкой

Зачет проводится с применением следующих методов: метод устного опроса по вопросам из перечня примерных вопросов из п. 5.2.

При необходимости предусматривается увеличение времени на подготовку к промежуточной аттестации. Процедура проведения промежуточной аттестации для обучающихся с ограниченными возможностями здоровья и обучающихся инвалидов устанавливается с учётом индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

5.2. Оценочные материалы промежуточной аттестации

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПКo2 OC-3	Способность принимать оптимальные управленческие решения с учетом критериев социально-экономической эффективности, рисков и возможностей использования имеющихся ресурсов	ПКo2 OC-3.1	Способность использовать программные продукты для формирования и анализа баз данных и правовой информации с целью обеспечения информационной безопасности

Описание показателей и критериев оценивания компетенции на различных этапах ее формирования

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
ПКo2 OC-3.1 Способность использовать программные продукты для формирования и анализа баз данных и правовой информации с целью	– Использует международные стандарты информационного обмена; дает определение понятия угрозы, защиты, видов противников или “нарушителей”; перечисляет модели безопасности и их применение; называет методы криптографии; называет методы и способы обеспечения информационной безопасности в профессиональной деятельности;	– Демонстрирует знаний основных теоретических положений в полном объеме

обеспечения информационной безопасности	идентифицирует информационные технологии в системе мер защиты информации; применяет нормативные документы по защите информации и организации соответствующих отделов в организациях; применяет руководящие документы, касающиеся государственной тайны.	
	– Демонстрирует способность самообучения в современных компьютерных средах; выделяет опасности и угрозы информационной безопасности; применяет основные методы и программы защиты информации; использует методы и способы обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты служебной информации.	– Применяет знания на практике в полной мере
	– Демонстрирует навыки криптографической и стеганографической защиты информации; применяет основные методы и средства защиты информации.	– Владеет навыками анализа и систематизации в выбранной сфере

Полный комплект оценочных материалов для промежуточной аттестации представлен в Приложении 1 РПД.

Типовые оценочные средства промежуточной аттестации

Вопросы к зачету по дисциплине «Основы информационной безопасности хозяйственной деятельности»

1. Понятие защиты информации и информационной безопасности.
2. Основные составляющие информационной безопасности.
3. Законодательный уровень информационной безопасности.
4. Компьютерные преступления.
5. Понятие атаки на информационную систему.
6. Классификация атак.
7. Виды противников или “нарушителей”, их классификация.
8. Каналы утечки информации.
9. Понятие угрозы.
10. Источники угроз и их классификация.
11. Модель угроз.
12. Анализ возможных способов нарушений информационной системы.
13. Политика безопасности и ее реализация.
14. Основные понятия криптографии.
15. Два основных направления в современной криптографии.
16. Классические криптосистемы и их классификация. Примеры.
17. Криптоанализ многоалфавитных систем.
18. Криптосистема: “Одноразовый блокнот”.
19. Стандарты шифрования данных.
20. Системы шифрования, не требующие передачи ключа.
21. Криптография с открытым ключом.
22. Электронная подпись и принципы ее применения.
23. Руководящие документы Гостехкомиссии России.
24. Инструкция СТР-К. Рекомендации по защите конфиденциальной информации.
25. Разрешительная система допуска.
26. Межсетевые экраны.
27. Технология VPN-сетей.
28. Угрозы информационной безопасности при работе с Интернет.
29. Архитектура типовой системы защиты от несанкционированного доступа.
30. Идентификация и аутентификация. Парольная аутентификация.

31. Подсистема управления доступом. Матрица доступа и списки доступа.
32. Программно-аппаратные средства защиты информации от НСД.
33. Устройства ввода идентификационных признаков.
34. Комплексный подход к обеспечению информационной безопасности организации.
35. Перспективы развития технологий обеспечения информационной безопасности.

Практические контрольные задания

Тема 1. Защита офисных документов.

Рассматриваемые вопросы:

Защита документов Microsoft Word от несанкционированного доступа.

Защита документов Microsoft Word от несанкционированного изменения.

Защита документов Microsoft Excel от несанкционированного изменения.

Защита документов Microsoft Excel от несанкционированного доступа.

Задания для самостоятельного выполнения:

Защита документов Word.

1. Создайте на диске D: в папке вашей группы папку Защита офиса.

2. Наберите в редакторе Word произвольный текст и сохраните его в папке Защита офиса под именем document1.

3. Выберите меню Сервис – Установить защиту.

4. Запретите любые изменения кроме записи исправлений и задайте пароль 12345.

5. Попробуйте отредактировать свой текст. Удалите некоторые слова и допишите новые.

Попробуйте принять все исправления (Сервис – Исправления – Принять/отклонить исправления). Обратите внимание, что все изменения в документе фиксируются, но принять/отклонить их невозможно.

6. Закройте документ, сохранив его.

7. Откройте документ и попробуйте принять исправления.

8. Снимите защиту документа. Выберите меню Сервис – Снять защиту и введите пароль.

9. Попробуйте принять все исправления. Убедитесь, что исправления приняты.

10. Заново защитите документ, кроме записи исправлений и закройте его, сохранив.

11. Наберите новый документ (отличный от первого) и сохраните его (под именем document2) в папке Защита офиса.

12. Установите защиту этого документа, выбрав меню Сервис – Установить защиту и запретив любые изменения кроме вставки примечаний. Задайте пароль 12345.

13. Попробуйте отредактировать документ.

14. Вставьте два примечания к любым фрагментам. Меню Вставка – Примечание.

15. Попробуйте изменить одно примечание и удалить другое.

16. Закройте документ, сохранив его.

17. Создайте третий документ в Word, сохраните его в папке Защита офиса под именем document3. Установите на него защиту, запретив любые изменения, кроме ввода данных в поля форм. Задайте пароль 12345.

18. Попробуйте отредактировать документ. Просмотрите пункты меню, чтобы выяснить Ваши возможности по редактированию документа.

19. Снимите защиту с документа.

20. Разбейте ваш документ на два раздела. (Установите курсор в место разрыва и выберите Меню Вставка – Разрыв – Новый раздел на текущей странице).

21. Установите защиту на документ, запретив любые изменения, кроме ввода данных в поля форм. Используя кнопку Разделы, установите запрет только на второй раздел. Пароль 12345.

22. Попробуйте отредактировать первый и второй разделы документа.

23. Закройте документ, сохранив его.

24. Создайте четвертый документ в редакторе Word и сохраните его в папке Защита офиса под именем document4.

25. Выберите меню Сервис – Параметры, затем вкладку Сохранение.

(Если Вы работаете в Word2t3 или XP, то надо выбрать вкладку Безопасность. Посмотрите возможности этой вкладки. Обратите внимание на флажок «Удалять личные сведения из файла при его сохранении»).

26. Задайте пароль 7777 на открытие файла.

27. Закройте файл, сохранив его, затем попробуйте открыть. Попробуйте ввести неправильный пароль, а затем откройте документ с правильным паролем.

28. Создайте пятый документ в редакторе Word и сохраните его в паке Защита офиса под именем document5.

29. Выберите меню Сервис – Параметры, затем вкладку Безопасность (Сохранение для Word2000) и задайте пароль разрешения записи 9999.

30. Закройте документ, сохранив его и попробуйте снова открыть. Выберите режим только чтения. Отредактируйте документ и попробуйте его сохранить. Сохраните как document5_1.

31. Попробуйте открыть файл document5_1.

32. Закройте все файлы и покажите результат преподавателю.

Защита документов Excel.

1. Запустите Excel и создайте следующую таблицу

ФИО	Оклад	Премия	Итого

2. Заполните ее для произвольных трех человек, вводя произвольные числа и суммируя их в графе Итого.

3. Постройте круговую диаграмму по столбцу Итого.

4. Сохраните файл в папке Защита офиса под именем proba1.

5. Сохраните этот же файл в папке Защита офиса еще раз под именем proba2.

6. Закройте файл proba2 и откройте файл proba1.

7. Выберите меню Сервис – Защита – Защитить лист и задайте пароль 1111.

8. Попробуйте отредактировать лист. Перейдите на Лист2 и попробуйте ввести данные.

9. Установите защиту второго листа с паролем 2222.

10. Снимите защиту с Листа1. Используйте меню Сервис – Защита – Снять защиту листа.

11. Установите защиту Листа1, отметив только флажок Защита листа в отношении объектов и задав пароль 1111.

12. Попробуйте изменить данные в ячейках. Попробуйте изменить диаграмму.

13. Закройте файл, сохранив его.

14. Откройте файл proba1 и попробуйте внести изменения на первый лист, затем на второй.

15. Закройте файл proba1 и откройте файл proba2.

16. Выберите меню Сервис – Защита – Защитить книгу. Оставьте отмеченным только флажок Структуру и задайте пароль kniga (проверьте, чтобы была включена английская раскладка)..

17. Попробуйте изменить данные на листе. Убедитесь, что изменения возможны.

18. Попробуйте удалить первый лист (пр. кнопка мыши на ярлыке листа внизу страницы).

19. Закройте файл, сохранив изменения, и заново откройте его (proba2).

20. Снимите защиту с книги. Меню Сервис – Защита – Снять защиту книги.

21. Установите защиту книги, отметив оба флажка и установив пароль kniga2.

22. Попробуйте изменить данные на листе.

23. Выберите меню Окно – Скрыть и введите пароль.

24. Закройте файл, сохранив изменения.

25. Откройте файл proba2. Убедитесь, что окно не отображается и данные не видны.

26. Выберите меню Окно – Отобразить и введите пароль.

27. Скройте окно и закройте файл, сохранив изменения.

28. Покажите результат преподавателю.

29. Снимите защиту со всех ваших файлов.

Литература:

www.microsoft.com

Лекционный материал.

Тема 2. Построение модели угроз.

Рассматриваемые вопросы:

Классификация атак.

Каналы утечки информации.

Понятие угрозы.

Источники угроз и их классификация.

Построение модели угроз.

Задания для самостоятельного выполнения:

Постройте модель угроз для некоторой организации, заполнив прилагаемую таблицу так, чтобы в ячейке стояла «1», если угроза, указанная в данной строке применима для объекта, указанного в данном столбце.

	Перечень источников угроз	Пути реализации	мониторы	Сист блоки	клавиатура	Принтеры	Копировально-множительные аппараты	магнитные носители инф-ции	Сеть электропитания	телефоны	Средства пожарной и охранный сигнализации
			1	2	3	4	5	6	7	8	9
Антропогенные источники угроз											
1	Интерес и преднамеренные действия криминальных структур и преступных группировок;	Утечка за счет агентов									
		Визуальная и фото разведка									
		Блокирование информации									
		Модификация информации									
		Уничтожение информации									
		Применение закладок									
2	Преднамеренные действия вспомогательного персонала (уборщики, охрана)	Регистрация наводок									
		Утечка информации									
		Визуальная и фото разведка									
		Блокирование информации									
		Модификация информации									
3	Ошибки пользователей	Уничтожение информации									
		Блокирование информации									
		Модификация информации									
4	Ошибки программистов	Уничтожение информации									
		Блокирование информации									
		Модификация информации									
Техногенные источники угроз											
5	Сбои в каналах передачи и средствах связи;	Блокирование информации									
		Уничтожение информации									
6	Сбои в средствах электропитания	Блокирование информации									
		Уничтожение информации									
7	Возможность аварий в инженерных	Блокирование информации									

	(водоснабжения, канализации) и коммуникационных сетях	Уничтожение информации											
Внешние стихийные источники													
8	Возможность ураганов	Уничтожение информации											
		Блокирование информации											
9	Возможность аварии близлежащих промышленных объектов	Уничтожение информации											
		Блокирование информации											
10	Возможность пожаров	Уничтожение информации											

Литература:

1. Лекционный материал.
2. Основы информационной безопасности хозяйственной деятельности: учебное пособие / И.П. Михнев; ВФ ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы». – Волгоград: Изд-во ВФ ФГБОУ ВПО РАНХиГС, 2013. – 144 с.
3. Платонов В. В. Программно-аппаратные средства защиты информации: учебник. / М.: Изд. центр "Академия". 2014.

Тема 3. Классические криптосистемы.

Рассматриваемые вопросы:

1. Классическая криптография.
2. Криптосистема Цезаря.
3. Криптосистема Виженера.
4. Практическая реализация системы Виженера.
5. Понятие многоалфавитной криптосистемы.
6. Криптоанализ многоалфавитной криптосистемы.
7. Криптоанализ системы Виженера.
8. Криптоанализ системы «Одноразовый блокнот».

Задания для самостоятельного выполнения:

1. Откройте файл CRYPTO1.XLS и посмотрите как реализована система Виженера.
2. Создайте в Excel следующую таблицу

Открытый текст					
Пароль					
Код букв текста					
Код букв пароля					
Сумма кодов букв					
Сумма по модулю					
Криптотекст					

3. Введите в первую строку произвольный текст по одной букве в каждую ячейку.
4. Введите во вторую строку таблицы произвольный пароль по одной букве в каждую ячейку. Если длина пароля меньше длины открытого текста, то начните набор пароля дальше, пока не закончится открытый текст.
5. Используя функцию КОДСИМВ, заполните четвертую и пятую строки таблицы для определения кодов каждой буквы открытого текста и пароля.
6. В пятой строке сложите третью и четвертую строки.
7. Если в пятой строке сумма превышает 255, то в шестой строке необходимо отнять 255 от числа в пятой строке. Используйте функцию ЕСЛИ.
8. В седьмой строке получите буквы зашифрованного текста, используя функцию СИМВОЛ.
9. Самостоятельно, используя описанные выше функции, расшифруйте полученный криптотекст. Для этого создайте ниже первой таблицы вторую таблицу.

10. Расшифруйте текст:

Ж С Я г з _ в Ц _ Ч Ц Ю б Х Ъ г _ Ц Ъ Я Ъ г ф г ж Ч Ш Я '

используя пароль «шифр». При наборе текста пропустите пробелы между буквами.

11. Расшифруйте текст:

Е Ы Я ж Ц С о _ Б в б У б д _ Щ ж _ У Ы з Ш Ф Ф _ Щ Щ а д _ Э п _ Э Э Ю б Э Р м н а к з
не зная пароля, но зная, что в зашифрованном тексте есть слово «истину».

Литература:

1. Лекционный материал.

2. Основы информационной безопасности хозяйственной деятельности: учебное пособие / И.П. Михнев; ВФ ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы». – Волгоград: Изд-во ВФ ФГБОУ ВПО РАНХиГС, 2013. – 144 с.

3. Платонов В. В. Программно-аппаратные средства защиты информации: учебник. / М.: Изд. центр "Академия". 2014.

Тема 4. Криптография с открытым ключом.

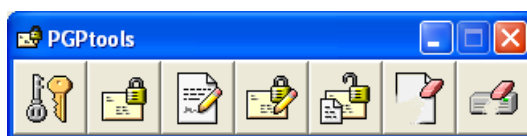
Рассматриваемые вопросы:

1. Криптография с открытым ключом.
2. Генерация ключевой пары в программе PGP.
3. Организация обмена ключами.
4. Шифрование данных в PGP.
5. Понятие электронной подписи.
6. Защита документов электронной подписью в программе PGP.
7. Шифрование и электронная подпись документов в PGP.


Задания для самостоятельного выполнения:

1. Запустите PGPtools (Пуск – Программы – PGP – PGPtools)


Появится панель




2. Выберите левую кнопку с двумя ключами. Запустится модуль PGPkeys со списком всех ключей на Вашем компьютере. В поле Description указано, какой это ключ: только открытый (public key) или ключевая пара, т.е. открытый и секретный ключ в комплекте (key pair).

3. Создайте новую ключевую пару, нажав на кнопку  и выполнив все шаги мастера создания ключей.

4. Создайте на диске D: папку с названием Вашей группы.


5. Экспортируйте свой открытый ключ в эту папку, нажав на кнопку  и указав путь до Вашей папки. В качестве названия файла с ключом укажите Вашу фамилию.

6. Скопируйте Ваш файл на сервер (Server606) в папку PublicKey.

7. Импортируйте из этой папки чьи-либо другие открытые ключи. Для этого нажмите на кнопку  и выберите путь и название файла.

8. Закройте окно PGPkeys.


9. Запустите Word и наберите письмо кому-либо, чей ключ вы импортировали. Сохраните этот текст в вашей папке.

10. Зашифруйте этот файл открытым ключом этого пользователя. Для этого нажмите кнопку  на панели PGPtools, укажите путь и название Вашего файла, а затем ключ в появившемся окне. Сохраните зашифрованный файл в Вашей папке под фамилией того, кому Вы писали.

11. Скопируйте этот файл на сервер (Server600) в папку TextPGP.


12. Скопируйте из этой папки в Вашу папку на диске D: файл, адресованный Вам.



13. Расшифруйте этот файл, нажав кнопку  или дважды щелкнув по нему мышкой, а затем выбрав Ваш ключ в списке ключей.

14. Создайте еще один документ в редакторе Word, сохранив его в Вашей папке на диске D:



15. Подпишите этот файл вашей электронной подписью. Для этого нажмите кнопку  на панели PGPtools, укажите путь и название Вашего файла, а затем Ваш ключ в появившемся окне.

16. Обратите внимание на файл подписи в вашей папке. Откройте его двойным щелчком.

17. Откройте подписанный Вами файл и измените его, сохранив изменения на диске.

18. Откройте файл подписи двойным щелчком еще раз. Убедитесь, что подпись не действительна.

19. Создайте новый документ в Word. Наберите небольшое предложение и скопируйте его в буфер обмена.



20. Щелкните мышкой по кнопке  на панели задач в правом нижнем углу.

21. В появившемся меню выберите Encrypt Clipboard и укажите Ваш ключ.

22. На чистом месте Вашего документа вставьте текст из буфера обмена (Правка – Вставить). Появился зашифрованный текст.

23. Скопируйте его в буфер обмена и по аналогии с шифрованием расшифруйте его, выбрав пункт Decrypt&Verify Clipboard.

24. Вставьте расшифрованный текст из буфера обмена.

Литература:

1. Лекционный материал.
2. Основы информационной безопасности хозяйственной деятельности: учебное пособие / И.П. Михнев; ВФ ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы». – Волгоград: Изд-во ВФ ФГБОУ ВПО РАНХиГС, 2013. – 144 с.
3. Платонов В. В. Программно-аппаратные средства защиты информации: учебник. / М.: Изд. центр "Академия". 2014.
4. Введение в криптографию/ Под общ. ред. В.В. Яценко. – М.: МЦНМО “ЧеРо”, 2013.
5. <http://pgp2all.org.ru>

Тема 5. Защита баз данных Microsoft Access.

Рассматриваемые вопросы:

1. Построение базы данных в Microsoft Access.
2. Защита базы данных от открытия.
3. Пользователи и группы.
4. Парольная защита.
5. Разграничение прав доступа.

Задания для самостоятельного выполнения:

1. Создайте на диске D: в папке вашей группы базу данных Секрет
2. Создайте таблицу в режиме конструктора (поле помеченное * является ключевым) и сохраните ее по имени Анкета.

	Имя поля	Тип данных
	Код	Счетчик
	ФИО	Текстовый
	Адрес	Текстовый
	Телефон	Текстовый

3. Введите в таблицу три записи.
4. Установите парольную защиту на эту базу данных (пароль 1234)
5. Создайте на диске D: в папке вашей группы базу данных Доступ.
6. Создайте для этой базы данных группы пользователей Student и Others
7. Создайте в группе Student пользователя под своей фамилией и пользователя Student1.

8. В группе Others создайте пользователя Friends и пользователя Guest.
9. Установите пароль администратору (admin) базы данных (**обязательно 7777**).
10. Установите пароли для созданных вами пользователей (пароли совпадают с именем пользователя).
11. Установите права доступа к базе данных для группы Student на все действия, кроме администрирования.
12. Установите права доступа к базе данных для группы Others только чтение и добавление данных.
13. Установите для группы Users права только на чтение данных и макета.
14. Покажите результат преподавателю.
15. Снимите пароль администратора

Литература:

1. Лекционный материал.
2. www.microsoft.com

Тема 6. Практическое применение межсетевых экранов.

Рассматриваемые вопросы:

1. Понятие межсетевого экрана.
2. Принципы работы с программой Firewall Outpost.
3. Настройка программных модулей.

Задания для самостоятельного выполнения:

Outpost Firewall

1. Загрузите программу Outpost Firewall.
2. Выберите пункт *Сетевая активность*. Окно справа содержит информацию о текущих соединениях приложений с сетью. Попробуйте получить информацию по какому-нибудь пункту.
3. Выберите пункт *Открытые порты*. Окно содержит информацию о том, какими процессами на компьютере открыты определенные порты.
4. Просмотрите пункты *Разрешенные* и *Заблокированные*, которые содержат общую статистику по соединениям.
5. Выберите пункт DNS. Кэширование запросов (т.е. сохранение ответов в базе Outpost) к DNS позволяет сократить время открытия страниц, которые были посещены ранее за счет того, что компьютеру не нужно будет перед открытием обращаться к DNS серверу для определения IP адреса открываемой страницы.
6. Просмотрите Журнал.
7. Щелкните правой кнопкой мыши по названию модуля DNS в левом окне программы и выберите *Параметры*.
8. Ограничьте кэш DNS на 50 записей и установите срок хранения 10 дней.
9. Выберите пункт *Детектор атак*, который хранит общую информацию о защите компьютера от атак, сканирования и других типов запрещенных соединений.
10. Просмотрите журнал. Щелкните правой кнопкой мыши по названию модуля *Детектор атак* в левом окне программы и выберите *Параметры*. В окне настроек при помощи ползунка можно выбрать один из трех уровней тревоги:
Максимальный – файрволл будет предупреждать о попытке подключения даже на один порт.
Обычный – предупреждение будет выдано только при сканировании с одного адреса нескольких портов или определенных портов, которые представляют определенный интерес.
Безразличный – файрволл будет сигнализировать лишь о реальной атаке на компьютер, а не о попытке исполнить такую атаку или просканировать порты.
11. Нажмите кнопку *Выбрать фильтр*. Просмотрите ее возможности.
12. Выберите пункт *Интерактивные элементы*. Здесь можно заблокировать всплывающие окна, переходы по рекламным сайтам в Интернет.

13. Просмотрите параметры настройки для данного пункта (правая кнопка мыши). На трех вкладках размещены настройки блокировки всех элементов, которые могут находиться на посещаемых веб-страницах или в почте. Большинство настроек имеют три настройки: *Разрешено*, *Запрос* и *Запрещено*. При настройке нужно учитывать тот факт, что на многих страницах скрипты или флэш могут использоваться для создания меню и если их полностью отключить, то навигация по сайту будет невозможна. Поэтому, оптимальным станет использование настройки *Запрос*. Для особой настройки некоторых сайтов в модуле *«Интерактивные элементы»* служит вкладка *«Исключения»*. С ее помощью можно сформировать список сайтов и настроить для каждого из них блокировку определенных элементов. Этот список имеет более высокий приоритет, чем общие настройки блокировки для всех сайтов.

14. Просмотрите вкладки параметров, запретите всплывающие окна и настройте остальное по своему усмотрению.

15. Выберите пункт *Реклама*. Outpost умеет отсекал рекламу по размеру и по содержимому ссылки, что экономит трафик и увеличивает скорость загрузки страниц.

16. Вызовите параметры для данного пункта (правая кнопка мыши). Установите флажок *Показать корзину для рекламы*. Если в стандартном списке отсутствует описание для определенного баннера, и он загружается при посещении страницы, то, открыв корзину, достаточно мышью перетащить в нее баннер, и он больше никогда не будет загружаться. Вкладка *Общие* позволяет выбрать то, чем будут заменяться вырезанные со страниц рекламные баннеры. Здесь же можно создать список сайтов, с которых не будет вырезаться графика и реклама.

17. Просмотрите все вкладки параметров.

18. Выберите пункт *Содержимое*. В настройках этого модуля можно задать список слов, которые могут встречаться на странице или в адресе страницы и которые будут служить Outpost–у сигналом того, что страницу отображать запрещено.

19. Просмотрите возможности данного пункта.

20. Выберите пункт *Фильтрация почтовых вложений*. В настройках этого модуля можно задать список типов файлов, которые подлежат переименованию, а так же включить вывод информационного сообщения о получении файлов определенного типа. Файл, тип которого указан в настройках этого модуля, при получении его почтовым клиентом, получит второе расширение *«.safe»*. Это позволит избежать автоматического выполнения почтовым клиентом кода, что может являться причиной заражения компьютера вирусами.

21. Просмотрите параметры данного пункта и его возможности.

22. Доступ к общим настройкам программы можно получить при помощи пункта меню *Параметры – Общие* из главного меню программы или нажатием соответствующей кнопки на панели. Вызовите окно настройки параметров и просмотрите вкладку *Общие*.

23. Вкладка *«Приложения»* позволяет управлять правилами поведения файрволла при попытке доступа в сеть определенных приложений. На этой вкладке перечислены все приложения, которые обнаружены на компьютере Outpost–ом при установке. Сразу после инсталляции эти приложения находятся в группе *«Пользовательский уровень»*. Для них создано одно или несколько правил, указывающих, каким образом приложение может обмениваться данными с сетью. Правило можно просмотреть или изменить при помощи двойного клика по имени его исполняемого файла.

24. Просмотрите правила для некоторых приложений.

25. Приложения из группы *Запрещенные приложения* никогда не получают доступа в сеть, вся их сетевая активность будет пресечена файрволлом. Некоторым приложениям можно полностью открыть доступ в сеть, переместив их в группу *«Доверенные приложения»*. Их доступ в сеть не ограничивается ничем, никакими правилами. Перемещение приложений из групп в группу, равно как и изменение правил, созданных для приложений, выполняется при помощи кнопки *Изменить*. При помощи кнопки *Добавить* можно внести в список новое приложение и затем создать для него правило общения с сетью.

26. Переместите приложение Excel в группу *Запрещенные приложения*.

27. Просмотрите оставшиеся вкладки настроек программы.

28. Попробуйте через сетевое окружение выйти на компьютер соседа.
29. Проверьте реакцию файрвола на попытку соседа обратиться к вашему компьютеру.
30. Перейдите в настройки общих параметров программы.
31. Выберите вкладку *Системные*. Уберите флажок NetBIOS. Теперь ваш компьютер недоступен по сети.
32. Дождитесь, когда ваш сосед выполнит предыдущее задание и попробуйте через сетевое окружение обратиться к его компьютеру.
33. Включите флажок NetBIOS на своем компьютере.
34. Вызовите журнал, нажав соответствующую кнопку на панели инструментов.
35. Просмотрите журнал.

Литература:

1. Лекционный материал.
2. Документация по работе с программой Firewall Outpost.
3. Основы информационной безопасности хозяйственной деятельности: учебное пособие / И.П. Михнев; ВФ ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы». – Волгоград: Изд-во ВФ ФГБОУ ВПО РАНХиГС, 2013. – 144 с.
4. Платонов В. В. Программно-аппаратные средства защиты информации: учебник. / М.: Изд. центр "Академия". 2014.

Тема 7. Защита информации в Интернет.

Рассматриваемые вопросы:

1. Принципы работы межсетевых экранов при работе с Интернет.
2. Настройка программных модулей при работе с Интернет.
3. Блокирование ненужного трафика и рекламы.

Задания для самостоятельного выполнения:

1. Загрузите программу Outpost Firewall.
2. Откройте в Internet Explorer страницу www.yandex.ru
3. Выберите пункт *Сетевая активность*. Просмотрите информацию о текущих соединениях с сетью.
4. Выберите пункт *Открытые порты*. Получите информацию о том, какими процессами на компьютере открыты определенные порты.
5. Просмотрите пункты *Разрешенные* и *Заблокированные*, которые содержат общую статистику по соединениям.
6. Выберите пункт DNS и в параметрах ограничьте кэш DNS на 50 записей и установите срок хранения 10 дней.
7. Выберите пункт *Детектор атак* и в параметрах задайте *Обычный* уровень тревоги.
8. Выберите пункт *Интерактивные элементы*. Просмотрите параметры настройки для данного пункта. На трех вкладках размещены настройки блокировки всех элементов, которые могут находиться на посещаемых веб–страницах или в почте. Настройте параметры по своему усмотрению (рекомендуется чаще использовать настройку *Запрос*).
9. Откройте в Internet Explorer страницу www.mail.ru, перейдите по какой-нибудь ссылке новостей.
10. Просмотрите в Outpost Firewall статистику по соединениям, а также статистику детектора атак.
11. Выберите пункт *Реклама*. Вызовите параметры для данного пункта. Установите флажок *Показать корзину для рекламы*.
12. Откройте стартовую страницу www.mail.ru и мышью перетащите в *Корзину для рекламы* рекламные баннеры с этой страницы.
13. Закройте страницу и попробуйте заново ее открыть. Проверьте, что происходит с рекламными баннерами.
14. Просмотрите все оставшиеся вкладки параметров.
15. Выберите пункт *Содержимое*. В настройках этого модуля можно задать список слов, которые могут встречаться на странице или в адресе страницы и которые будут служить Outpost–у сигналом того, что страницу отображать запрещено.

16. Настройте программу так, чтобы Outpost блокировал все страницы, в адресе которых присутствует слово chat. Попробуйте открыть страницу www.chat.ru.

17. Выберите пункт *Фильтрация почтовых вложений*. В настройках этого модуля можно задать список типов файлов, которые подлежат переименованию, а так же включить вывод информационного сообщения о получении файлов определенного типа.

18. Задайте вывод информационного сообщения для всех файлов с расширением .zip и переименование файлов с расширением .exe.

19. Покажите результат преподавателю.

20. Отмените все свои настройки и закройте все открытые приложения.

Литература:

1. Лекционный материал.
2. Основы информационной безопасности хозяйственной деятельности: учебное пособие / И.П. Михнев; ВФ ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы». – Волгоград: Изд-во ВФ ФГБОУ ВПО РАНХиГС, 2013. – 144 с.
3. Платонов В. В. Программно-аппаратные средства защиты информации: учебник. / М.: Изд. центр "Академия". 2014.

Тема 8. Типовая структура защиты от НСД. Управление доступом.

Рассматриваемые вопросы:

1. Типовая структура защиты информации от НСД.
2. Подсистема управления доступом.
3. Построение матрицы доступа.
4. Документация отдела обеспечения информационной безопасности.

Задания для самостоятельного выполнения:

1. Рассмотрите типовую структуру защиты информации от НСД.
2. Продумайте структуру защиты информации от НСД для произвольной (вымышленной) организации.
3. Рассмотрите подсистему управления доступом для этой организации.
4. Составьте перечень защищаемых информационных ресурсов организации.
5. Постройте матрицу доступа для данной организации.
6. Составьте документ, определяющий правила доступа пользователей к ресурсам при помощи личных идентификаторов и паролей, правила составления, смены и хранения паролей.
7. Сохраните все документы в своей личной папке (и на своей дискете).

Литература:

1. Лекционный материал.
2. Основы информационной безопасности хозяйственной деятельности: учебное пособие / И.П. Михнев; ВФ ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы». – Волгоград: Изд-во ВФ ФГБОУ ВПО РАНХиГС, 2013. – 144 с.

Шкала оценивания

Уровень знаний, умений и навыков обучающегося при устном ответе во время промежуточной аттестации определяется оценками «зачтено» или «незачтено». Критериями оценивания на зачете является демонстрация основных теоретических положений, в рамках осваиваемой компетенции, умение применять полученные знания на практике. Для дисциплин, формой итогового отчета которых является зачет, приняты следующие соответствия:

60% - 100% - «зачтено»;

менее 60% - «не зачтено».

При оценивании результатов устного опроса используется следующая шкала оценок:

100% - 90% (отлично)	Этапы компетенции, предусмотренные образовательной программой, сформированы на высоком уровне. Свободное владение материалом, выявление межпредметных связей. Уверенное владение понятийным аппаратом дисциплины. Практические навыки профессиональной деятельности сформированы на высоком уровне. Способность к самостоятельному нестандартному решению практических задач
89% - 75% (хорошо)	Этапы компетенции, предусмотренные образовательной программой, сформированы достаточно. Детальное воспроизведение учебного материала. Практические навыки профессиональной деятельности в значительной мере сформированы. Присутствуют навыки самостоятельного решения практических задач с отдельными элементами творчества.
74% - 60% (удовлетворительно)	Этапы компетенции, предусмотренные образовательной программой, сформированы на минимальном уровне. Наличие минимально допустимого уровня в усвоении учебного материала, в т.ч. в самостоятельном решении практических задач. Практические навыки профессиональной деятельности сформированы не в полной мере.
менее 60% (неудовлетворительно)	Этапы компетенции, предусмотренные образовательной программой, не сформированы. Недостаточный уровень усвоения понятийного аппарата и наличие фрагментарных знаний по дисциплине. Отсутствие минимально допустимого уровня в самостоятельном решении практических задач. Практические навыки профессиональной деятельности не сформированы.

Процедура оценивания результатов обучения, характеризующих этапы формирования компетенций, осуществляются в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации студентов в ФГБОУ ВО РАНХиГС и Регламентом о балльно-рейтинговой системе в Волгоградском институте управления - филиале РАНХиГС.

6. Методические материалы по освоению дисциплины

Методические рекомендации по написанию рефератов

Реферат является индивидуальной самостоятельно выполненной работой студента. Тему реферата студент выбирает из перечня тем, рекомендуемых преподавателем, ведущим соответствующую дисциплину. Реферат должен содержать следующие структурные элементы: Титульный лист Содержание Введение Основная часть Заключение Список литературы Приложения (при необходимости). Требования к оформлению рефератов: шрифт – 14, поля – по 2 см, интервал – 1, объем – не менее 10 стр.

Методические указания для обучающихся по освоению дисциплины

При работе с настоящим учебно-методическим комплексом особое внимание следует обратить на знание теоретических вопросов информатики, иметь высокий уровень информационной культуры, знать устройство современного персонального компьютера, иметь глубокие навыки работы с современными операционными системами и офисными прикладными пакетами. Перед выполнением практических заданий обязательно должен быть подробно разобран и изучен теоретический материал по каждой теме курса.

В процессе изучения курса студент должен выработать навыки и приемы владения современными технологиями обработки, хранения, передачи и приема массивов юридической информации в различных областях деятельности практика-юриста и уметь их использовать в современном рыночном мире.

Для более углубленного изучения дисциплины, самостоятельной разработке докладов, сообщений в т.ч. с использованием мультимедийных средств, либо выполнении практической работы студентам необходимо пользоваться рекомендованной в рабочей программе литературой. При самостоятельном изучении курса рекомендуется пользоваться источниками, указанными в списке основной литературы.

Структура времени, необходимого на изучение дисциплины

Форма изучения дисциплины	Время, затрачиваемое на изучение дисциплины, %
Изучение литературы, рекомендованной в учебной программе	40
Решение задач, практических упражнений и ситуационных примеров	40
Изучение тем, выносимых на самостоятельное рассмотрение	20
Итого	100

Рекомендации по подготовке к практическому (семинарскому) занятию

Практическое (семинарское) занятие - одна из основных форм организации учебного процесса, представляющая собой коллективное обсуждение студентами теоретических и практических вопросов, решение практических задач под руководством преподавателя. Основной целью практического (семинарского) занятия является проверка глубины понимания студентом изучаемой темы, учебного материала и умения изложить его содержание ясным и четким языком, развитие самостоятельного мышления и творческой активности у студента. На практических (семинарских) занятиях предполагается рассматривать наиболее важные, существенные, сложные вопросы, которые наиболее трудно усваиваются студентами. При этом готовиться к практическому (семинарскому) занятию всегда нужно заранее. Подготовка к практическому (семинарскому) занятию включает в себя следующее:

- обязательное ознакомление с планом занятия, в котором содержатся основные вопросы, выносимые на обсуждение;
- изучение конспектов лекций, соответствующих разделов учебника, учебного пособия, содержания рекомендованных нормативных правовых актов;
- работа с основными терминами (рекомендуется их выучить);
- изучение дополнительной литературы по теме занятия, делая при этом необходимые выписки, которые понадобятся при обсуждении на семинаре;
- формулирование своего мнения по каждому вопросу и аргументированное его обоснование;
- запись возникших во время самостоятельной работы с учебниками и научной литературы вопросов, чтобы затем на семинаре получить на них ответы;
- обращение за консультацией к преподавателю.

Практические (семинарские) занятия включают в себя выполнение заданий на компьютере по какой-либо сложной или особо актуальной проблеме, решение задач. На практическом (семинарском) занятии студент проявляет свое знание предмета, корректирует информацию, полученную в процессе лекционных и внеаудиторных занятий, формирует определенный образ в глазах преподавателя, получает высокие навыки освоения информационных технологий применительно в профессиональной сфере, навыки практического решения задач на компьютере.

Методические рекомендации по написанию семестровой контрольной работы

Контрольная работа является индивидуальной самостоятельно выполненной работой студента. Вариант контрольной работы студент выбирает из перечня работ, рекомендуемых преподавателем, ведущим данную дисциплину. Контрольная работа, как правило, должна содержать следующие структурные элементы: Титульный лист Содержание Введение Основная часть Заключение Список литературы Приложения (при необходимости).

Требования к объему: не более 15 страниц. Оформление: Шрифт TimesNewRoman, 12 шрифт, 1,5 интервала, 1,5 см абзацный отступ. Оригинальность по системе Антиплагиат.ВУЗ – не менее 60 процентов.

Рекомендации по изучению методических материалов

Методические материалы по дисциплине позволяют студенту оптимальным образом организовать процесс изучения данной дисциплины. Методические материалы по дисциплине призваны помочь студенту понять специфику изучаемого материала, а в конечном итоге – максимально полно и качественно его освоить. В первую очередь студент должен осознать предназначение методических материалов: структуру, цели и задачи. Для этого он знакомится с преамбулой, оглавлением методических материалов, говоря иначе, осуществляет первичное знакомство с ним. В разделе, посвященном методическим рекомендациям по изучению дисциплины, приводятся советы по планированию и организации необходимого для изучения дисциплины времени, описание последовательности действий студента («сценарий изучения дисциплины»), рекомендации по работе с литературой, советы по подготовке к экзамену и разъяснения по поводу работы с тестовой системой курса и над домашними заданиями. В целом данные методические рекомендации способны облегчить изучение студентами дисциплины и помочь успешно сдать экзамен. В разделе, содержащем учебно-методические материалы дисциплины, содержание практических занятий по дисциплине, словарь основных терминов дисциплины.

Неотъемлемым элементом учебного процесса является самостоятельная работа студента. При самостоятельной работе достигается конкретное усвоение учебного материала, развиваются теоретические способности, столь важные для современной подготовки специалистов. Формы самостоятельной работы студентов по дисциплине: написание конспектов, подготовка ответов к вопросам, написание рефератов, решение задач, исследовательская работа, выполнение контрольной работы.

Рекомендации по самостоятельной работе студентов

На самостоятельную работу студентов по дисциплине «**Основы информационной безопасности хозяйственной деятельности**» выносятся следующие темы:

№ п/п	Тема	Вопросы, выносимые на СРС	Очная форма	Заочная форма
1	2	3	4	5
1.	Понятие информации, защиты информации и информационной безопасности. Основные составляющие.	Понятие информации, защиты информации и информационной безопасности. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства, на уровне региона и на локальном уровне. Основные положения теории информационной безопасности информационных систем.	0	0
2.	Законодательный уровень информационной безопасности. Компьютерные преступления. Ответственность за совершение компьютерных преступлений.	Обзор российского законодательства в области обеспечения информационной безопасности. Доктрина информационной безопасности РФ, законы «О государственной тайне», «Об информации, информационных технологиях и о защите информации». Основные нормативные руководящие документы, касающиеся государственной тайны и конфиденциальной информации. Нормативные акты администрации Волгограда в области информационной безопасности.	0	0
3.	Классификация атак. Понятие угрозы. Модель угроз. Рекомендации по обеспечению информационной безопасности.	Понятие атаки на информационную систему. Классификация атак. Виды противников или «нарушителей», их классификация. Каналы утечки информации: визуально-оптический, акустический, электромагнитный и материально-вещественный. Понятие угрозы. Источники угроз и их классификация. Построение модели угроз организации. Примеры. Специальные требования и рекомендации. Показатели защищенности.	0	0

		Система защиты информации от несанкционированного доступа. Рекомендуемые меры по обеспечению защиты информации в процессе эксплуатации информационной системы. Разрешительная система допуска.		
4.	Основные понятия криптографии. Два современных направления в криптографии. Классические криптосистемы.	Стеганография и криптография. Важность криптографии при решении задач обеспечения информационной безопасности хозяйственной деятельности и сохранения конфиденциальной информации. Основные понятия криптографии. Понятие криптосистемы, ключа. Возможные атаки на криптосистемы, понятие криптоанализа. Надежность криптосистемы. Два основных направления в современной криптографии. Одноалфавитные и многоалфавитные криптосистемы. Системы Цезаря и Виженера. Возможности криптоанализа многоалфавитных систем. Раскрытие системы Виженера. Надежность многоалфавитных систем. Абсолютно надежная криптосистема: “Одноразовый блокнот”. Криптосистема DES.	0	0
5	Криптография с открытым ключом. Системы шифрования, не требующие передачи ключа. Электронная подпись.	Системы шифрования, не требующие передачи ключа. Протокол использования системы «Одноразовый блокнот», не требующий первоначального обмена секретными ключами. Криптография с открытым ключом. Понятие открытого и секретного ключа. Принципы построения криптосистем с открытым ключом. Известные криптосистемы с открытым ключом и их алгоритмы. Система RSA. Длина ключа в криптографии с открытым ключом. Односторонняя функция, возможность ее использования. Электронная подпись и принципы ее применения.	0	0
6	Основные технологии построения защищенных ИС. Межсетевые экраны.	Основные технологии построения защищенных ИС. Понятие межсетевого экрана. Правила фильтрации и принципы их применения. Пакетные фильтры. Политика сетевой безопасности. Политика реализации межсетевых экранов. Функциональные требования к межсетевым экранам и их компоненты. Шлюзы сеансового и прикладного уровня. Новые функции брандмауэров. Схемы организации межсетевых экранов. Требования к межсетевым экранам	0	0
7	Технология VPN-сетей.	Технология объединения локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи данных в единую виртуальную сеть, обеспечивающую защиту информационных потоков или технология VPN-сетей. Особенности VPN. Туннелирование и его особенности. Основные разновидности VPN-устройств по технической реализации. Роли VPN-устройств. Варианты построения защищенных каналов VPN. Угрозы для VPN. Классификация VPN-сетей. Совмещение VPN-технологий и межсетевого экрана. Недостатки VPN.	0	0
8	Защита информации в Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей.	Проблема обеспечения информационной безопасности при работе с глобальной сетью Интернет. Информационная безопасность в условиях функционирования в России глобальных сетей. Указ президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена». Угрозы информационной безопасности при работе с Интернет. Вирусы, исполняемые модули, всплывающие окна и реклама. Использование антивирусных программ и межсетевых экранов при работе	0	0

		с Интернет. Программные средства проверки трафика и борьбы с несанкционированным использованием ресурсов информационной системы.		
9	Типовая структура защиты от НСД. Управление доступом.	Архитектура типовой системы защиты от несанкционированного доступа. Идентификация и аутентификация. Парольная аутентификация. Правила применения паролей. Одноразовые пароли. Принципы контроля доступа. Матрица доступа и списки доступа. Произвольное и принудительное управление доступом. Ограничивающий интерфейс. Ролевое управление доступом. Криптографическая подсистема. Программно-аппаратные средства защиты информации от НСД. Устройства ввода идентифицируемых признаков. Преимущества и недостатки их использования. Электронные замки.	О, Т	О, Т

Неотъемлемым элементом учебного процесса является самостоятельная работа студента. При самостоятельной работе достигается конкретное усвоение учебного материала, развиваются теоретические способности, столь важные для современной подготовки специалистов. Формы самостоятельной работы студентов по дисциплине: написание конспектов, подготовка ответов к вопросам, написание рефератов, решение задач, исследовательская работа, выполнение контрольной работы.

Задания для самостоятельной работы включают в себя комплекс аналитических заданий выполнение, которых, предполагает тщательное изучение научной и учебной литературы, периодических изданий, а также законодательных и нормативных документов предлагаемых в п. 7.4 «Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет», учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине». Задания предоставляются на проверку в печатном виде.

Рекомендации по работе с литературой

При изучении курса учебной дисциплины особое внимание следует обратить на рекомендуемую основную и дополнительную литературу.

Важным элементом подготовки к семинару является глубокое изучение основной и дополнительной литературы, рекомендованной по теме занятия, а также первоисточников. При этом полезно прочитанную литературу законспектировать. Конспект должен отвечать трем требованиям: быть содержательным, по возможности кратким и правильно оформленным.

Содержательным его следует считать в том случае, если он передает все основные мысли авторов в целостном виде. Изложить текст кратко – это значит передать содержание книги, статьи в значительной мере своими словами. При этом следует придерживаться правила - записывать мысль автора работы лишь после того, как она хорошо понята. В таком случае поставленная цель будет достигнута. Цитировать авторов изучаемых работ (с обязательной ссылкой на источник) следует в тех случаях, если надо записывать очень важное определение или положение, обобщающий вывод.

Важно и внешнее оформление конспекта. В его начале надо указать тему семинара, дату написания, названия литературных источников, которые будут законспектированы. Глубокая самостоятельная работа над ними обеспечит успешное усвоение изучаемой дисциплины.

Одним из важнейших средств серьезного овладения теорией является **конспектирование первоисточников**.

Для составления конспекта рекомендуется сначала прочитать работу целиком, чтобы уяснить ее общий смысл и содержание. При этом можно сделать пометки о ее структуре, об основных положениях, выводах, надо стараться отличать в тексте основное от второстепенного, выводы от аргументов и доказательств. Если есть непонятные слова, надо в энциклопедическом словаре найти, что это слово обозначает. Закончив чтение (параграфа, главы, статьи) надо задать себе вопросы такого рода: В чем главная мысль? Каковы основные звенья доказательства ее? Что

вытекает из утверждений автора? Как это согласуется с тем, что уже знаете о прочитанном из других источников?

Ясность и отчетливость восприятия текста зависит от многого: от сосредоточенности студента, от техники чтения, от настойчивости, от яркости воображения, от техники фиксирования прочитанного, наконец, от эрудиции – общей и в конкретно рассматриваемой проблеме.

Результатом первоначального чтения должен быть простой *план текста и четкое представление о неясных местах*, отмеченных в книге. После предварительного ознакомления, при повторном чтении следует *выделить основные мысли автора* и их развитие в произведении, обратить внимание на обоснование отдельных положений, на методы и формы доказательства, наиболее яркие примеры. В ходе этой работы окончательно отбирается материал для записи и определяется ее вид: *план, тезисы, конспект*.

План это краткий, последовательный перечень основных мыслей автора. Запись прочитанного в виде тезисов – это выявление и запись опорных мыслей текста. Разница между планом и тезисами заключается в следующем: в плане мысль называется (ставь всегда вопрос: о чем говорится?), в тезисах – формулируется – (что именно об этом говорится?). Запись опорных мыслей текста важна, но полного представления о прочитанном на основании подобной записи не составишь. Важно осмыслить, как автор доказывает свою мысль, как убеждает в истинности своих выводов. Так возникает конспект. Форма записи, как мы уже отметили, усложняется в зависимости от целей работы: план – о чем?; тезисы – о чем? что именно?; конспект – о чем? что именно? как?

Конспект – это краткое последовательное изложение содержания. Основу его составляет план, тезисы и выписки. Недостатки конспектирования: многословие, цитирование не основных, а связующих мыслей, стремление сохранить стилистическую связанность текста в ущерб его логической стройности. Приступать к конспектированию необходимо тогда, когда сложились навыки составления записи в виде развернутого подробного плана.

Форма записи при конспектировании требует особого внимания: важно, чтобы собственные утверждения, размышления над прочитанным, четко отделялись при записи. Разумнее выносить свои пометки на широкие поля, записывать на них дополнительные справочные данные, помогающие усвоению текста (дата события, упомянутого авторами; сведения о лице, названном в книге; точное содержание термина). Если конспектируется текст внушительного объема, необходимо указывать страницы книги, которые охватывает та или иная часть конспекта.

Для удобства пользования своими записями важно озаглавить крупные части конспекта, подчеркивая *заголовки*. Следует помнить о назначении красной строки, стремиться к четкой графике записей – уступами, колонками. Излагать главные мысли автора и их систему аргументов необходимо преимущественно своими словами, перерабатывая таким образом информацию, – так проходит уяснение ее сути. Мысль, фразы, понятия в контексте, могут приобрести более пространное изложение в записи. Но текст оригинала свертывается, и студент, отрабатывая логическое мышление, учится выделять главное и обобщать однотипные суждения, однородные факты. Кроме того, делая записи своими словами, обобщая, студент учится письменной речи.

Знание общей стратегии чтения, техники составления плана и тезисов определяет и технологию конспектирования:

- внимательно читать текст, попутно отмечая непонятные места, незнакомые термины и понятия. *Выписать на поля* значение отмеченных понятий.
- при первом чтении текста необходимо составить его *простой план*, последовательный перечень основных мыслей автора.
- при повторном чтении текста выделять *систему доказательств* основных положений работы автора.
- заключительный этап работы с текстом состоит в осмыслении ранее отмеченных мест и их краткой последовательной записи.
- при конспектировании нужно стремиться *выразить мысль автора своими словами*, это помогает более глубокому усвоению текста.

- в рамках работы над первоисточником важен умелый *отбор цитат*. Необходимо учитывать, насколько ярко, оригинально, сжато изложена мысль. Цитировать необходимо те суждения, на которые впоследствии возможна ссылка как на авторитетное изложение мнения, вывода по тому или иному вопросу.

Конспектировать целесообразно не на отдельном листе, а в общей тетради на одной странице листа. Обратная сторона листа может быть использована для дополнений, необходимость которых выяснится в дальнейшем. При конспектировании литературы следует оставить широкие поля, чтобы записать на них план конспекта. Поля могут быть использованы также для записи своих замечаний, дополнений, вопросов. При выступлении на семинаре студент может пользоваться своим конспектом для цитирования первоисточника. Все обучающиеся внимательно слушают выступления одногруппников, отмечают спорные или ошибочные положения в них, вносят поправки, представляют свои решения и обоснования обсуждаемых проблем.

В конце семинара, когда преподаватель подводит итоги занятия, студенты с учетом рекомендаций преподавателя и выступлений сокурсников дополняют или исправляют свои конспекты.

Особенности изучения дисциплины студентами заочной форм обучения

Студенты заочной форм обучения изучают отдельные наиболее значимые темы дисциплины, согласно отведенным по учебному плану часам, под руководством преподавателя в ходе аудиторных занятий. Остальные темы дисциплины студенты изучают самостоятельно. В ходе самостоятельной работы студенты пишут контрольную работу по одной из предложенных преподавателем тем. В ходе зачетно-экзаменационной сессии студенты представляют контрольную работу для оценки. Наличие положительной оценки является допуском к сдаче зачета по дисциплине.

Практические (семинарские) занятия включают в себя и специально подготовленные рефераты, выступления по какой-либо сложной или особо актуальной проблеме, решение задач. На практическом (семинарском) занятии студент проявляет свое знание предмета, корректирует информацию, полученную в процессе лекционных и практических занятий, формирует определенный образ в глазах преподавателя, получает навыки практической работы на компьютере, навыки практического решения задач.

При проведении занятий следует уделять внимание теоретическим вопросам, особенно по сложным темам. Теоретические вопросы рассматриваются либо самостоятельно, либо в связи с решением конкретных задач. Обсуждение теоретических вопросов заставит студентов не только готовить решение задач, но и готовить тему в целом. Теоретическим вопросам целесообразно уделять до 15-20 минут. При необходимости теоретическим вопросам может быть посвящена большая часть занятия.

Задаваемые студентам задачи и теоретические вопросы для обсуждения на практических занятиях должны тщательно продумываться, с тем, чтобы охватить по возможности все важные аспекты темы. Количество задаваемых задач зависит от темы и сложности решения, но обычно составляет не менее 3-4.

Рекомендации по подготовке к промежуточной аттестации

К сдаче зачета по дисциплине допускаются студенты, получившие не меньше 60 баллов при текущей аттестации. При подготовке к зачету студент внимательно просматривает вопросы, предусмотренные в рабочей программе, и продолжает знакомиться с рекомендованной литературой. Основой для сдачи зачета студентом является изучение конспектов обзорных лекций, прослушанных в течение семестра, информации полученной в результате самостоятельной работы и получение практических навыков при решении задач в течение семестра.

Фундамент любого учебного курса закладывается на лекционных и практических занятиях, а также при подготовке к ним. Необходимо выработать серьезное отношение к конспекту лекций, который должен в полном объеме отражать содержание лекций. Записи должны быть аккуратными. Желательно особо выделить все определения и ключевые моменты

лекции. Особо следует отметить, что, несмотря на практическую направленность семинаров и выполнение всех заданий на компьютере, студентам необходимо самостоятельно записывать ключевые моменты заданий в конспект, дополняя лекции. В случае недопонимания некоторых моментов необходимо обязательно обращаться к преподавателю за консультацией.

Для более успешного освоения материала необходимо использовать дополнительную литературу. Учебник нужно не просто читать, а изучать; основой запоминания является только понимание прочитанного. Необходимо выработать привычку систематической самостоятельной работы, «натаскивание» к экзамену или зачету дает слабый и поверхностный результат.

Для успешной сдачи зачета студент должен знать и понимать достаточно солидный объем материала. Не откладывайте процесс заучивания на последние дни перед зачетом. Подготовка должна вестись с первых лекций.

7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

7.1. Основная литература

1. Основы информационной безопасности хозяйственной деятельности: учебное пособие / И.П. Михнев; ВФ ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы». – Волгоград: Изд-во ВФ ФГБОУ ВПО РАНХиГС, 2013. – 144 с.
2. Платонов В. В. Программно-аппаратные средства защиты информации: учебник. / М.: Изд. центр "Академия". 2014.
3. Малюк, А.А. Введение в информационную безопасность: учебное пособие. Горячая линия-Телеком.2011. Режим доступа: <http://www.iprbookshop.ru/11979>.- ЭБС «IPRbooks»
4. Канивец Е.К. Информационные технологии в профессиональной деятельности [Электронный ресурс]: курс лекций. Оренбург: Оренбургский государственный университет, ЭБС АСВ. 2015. Режим доступа: <http://www.iprbookshop.ru/54115>. — ЭБС «IPRbooks»,
5. Литвинов В.А. Информационные технологии в юридической деятельности: учеб. пособие. СПб.: Питер. 2013. - 320 с.
6. ЭБС Лань <http://lib.ranepa.ru/base/abs-izdatelstva--lan-.html#>
7. ЭБС IPRbooks <http://lib.ranepa.ru/base/abs-iprbooks.html>
8. Электронное издательство «ЮРАЙТ» <http://www.biblio-online.ru>

7.2. Дополнительная литература

1. Кузнецов И.Н. Бизнес-безопасность [Электронный ресурс]: учебное пособие. М.: Дашков и К. 2012. Режим доступа: <http://www.iprbookshop.ru/10906>.— ЭБС «IPRbooks»
2. ЭБС Лань <http://lib.ranepa.ru/base/abs-izdatelstva--lan-.html#>
3. ЭБС IPRbooks <http://lib.ranepa.ru/base/abs-iprbooks.html>
4. Электронное издательство «ЮРАЙТ» <http://www.biblio-online.ru>
5. Доктрина информационной безопасности РФ (утв. Президентом РФ 09.09.2000).
6. Закон РФ “О государственной тайне” № 5485-1 от 21.07.1993 г.
7. Закон РФ “Об информации, информационных технологиях и о защите информации” № 149-ФЗ от 27.07.2006
8. Закон РФ “О коммерческой тайне” № 98-ФЗ от 29.07.2004 г.
9. Блэк У. Интернет: протоколы безопасности: Учебный курс. СПб.: Питер-пресс, 2012.
10. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. СПб: БХВ-Петербург, 2014.
11. Компьютерная преступность и информационная безопасность /Под общ. ред. А. П. Леонова. Мн.: АРИЛ, 2014.
12. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. СПб.: Издательство «Лань», 2013.

7.3. Нормативные правовые документы и иная правовая информация

1. Конституция Российской Федерации от 12.12.1993 (с посл. поправками)

2. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
3. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
4. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781;
5. Порядок проведения классификации информационных систем персональных данных, утвержденный приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20 (зарегистрирован Минюстом России 3 апреля 2008 года, регистрационный № 11462);
6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.);
7. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 14 февраля 2008г.).
8. Закон РФ «О государственной тайне» № 5485-1 от 21.07.1993 г.
9. Закон РФ «О коммерческой тайне» № 98-ФЗ от 29.07.2004 г.

7.4. Интернет-ресурсы, справочные системы

1. <http://base.garant.ru/> - справочно-поисковая система «Гарант»
2. <http://www.consultant.ru/> - справочно-поисковая система «Консультант Плюс»
3. <http://www.pfrf.ru/> - официальный сайт Пенсионного фонда РФ
4. <http://www.kremlin.ru/> - официальный сайт Президента РФ
5. <http://www.cbr.ru/> - официальный сайт Центрального банка РФ
6. Официальный сайт Государственной Думы РФ - duma.gov.ru
7. Официальный сайт Правительства Волгоградской области - volganet.ru
8. Официальный сайт Правительства РФ - pravительство.рф
9. Официальный сайт Совета Федерации - council.gov.ru

7.5. Иные источники

Нет

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

Материально-техническое обеспечение дисциплины «**Основы информационной безопасности хозяйственной деятельности**» включает в себя:

- лекционные аудитории, оборудованные видеопроекционным оборудованием для презентаций, средствами звуковоспроизведения, экраном;
- помещения для проведения семинарских и практических занятий, оборудованные учебной мебелью;
- компьютерные классы, оснащенные современными компьютерами с выходом в Интернет и установленными в сети специальными пакетами программ, обеспечивающими учебный процесс, включая СПС Консультант Плюс и Гарант.

Дисциплина должна быть поддержана соответствующими лицензионными программными продуктами: Microsoft Windows 7 Prof, Microsoft Office 2010, Kaspersky 8.2, СПС Гарант, СПС Консультант.

Программные средства обеспечения учебного процесса включают:

- операционные системы семейства Windows (10): Microsoft WINHOME 10 RUS OLP NL AcdmcLegalizationGetGenuine, Microsoft WinPro 10 RUSUpgrdOLPNLAcdmc;
- пакет офисного ПО - Microsoft OfficeStd 2019 RUS OLP NL Acdmc;
- программы-архиваторы;
- антивирусные программы;

- программы презентационной графики;
- текстовые редакторы;
- графические редакторы;
- электронная таблица;
- база данных;
- СПС Консультант Плюс;
- СПС Гарант Аэро;
- электронная библиотека;
- программа электронного тестирования.

Вуз обеспечивает каждого обучающегося рабочим местом в компьютерном классе в соответствии с объемом изучаемых дисциплин, обеспечивает выход в сеть Интернет и доступ к СПС Консультант Плюс и СПС Гарант.

Материально-техническое обеспечение дисциплины для обучающихся с ограниченными возможностями здоровья и инвалидов включает в себя следующее:

- учебные аудитории оснащены специальным оборудованием и учебными местами с техническими средствами обучения для обучающихся с различными видами ограничений здоровья;

- учебная аудитория, в которой обучаются студенты с нарушением слуха оборудована компьютерной техникой, аудиотехникой (акустический усилитель и колонки), видеотехникой (мультимедийный проектор), мультимедийной системой. Для обучения лиц с нарушениями слуха используются мультимедийные средства и другие технические средств для приема-передачи учебной информации в доступных формах;

- для слабовидящих обучающихся в лекционных и учебных аудиториях предусмотрен просмотр удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра;

- для обучающихся с нарушениями опорно-двигательного аппарата в лекционных и учебных аудиториях предусмотрены специально оборудованные рабочие места;

- для контактной и самостоятельной работы используется мультимедийные комплексы, электронные учебники и учебные пособия, адаптированные к ограничениям здоровья обучающихся.

Обучающиеся с ограниченными возможностями здоровья и инвалиды, в отличие от остальных, имеют свои специфические особенности восприятия, переработки материала, выполнения промежуточных и итоговых форм контроля знаний. Они обеспечены печатными и электронными образовательными ресурсами (программы, учебники, учебные пособия, материалы для самостоятельной работы и т. д.) в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,

Для лиц с нарушениями слуха, с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

Вуз обеспечивает каждого обучающегося рабочим местом в компьютерном классе в соответствии с объемом изучаемых дисциплин, обеспечивает выход в сеть Интернет.

Помещения для самостоятельной работы обучающихся включают следующую оснащенность: столы аудиторные, стулья, доски аудиторные, компьютеры с подключением к локальной сети института (включая правовые системы) и Интернет.

Для изучения учебной дисциплины используются автоматизированная библиотечная информационная система и электронные библиотечные системы: «Университетская библиотека ONLINE», «Электронно-библиотечная система издательства ЛАНЬ», «Электронно-библиотечная система издательства «Юрайт», «Электронно-библиотечная система IPRbooks», «Научная электронная библиотека eLIBRARY» и др.

Обеспечивается возможность беспрепятственного доступа обучающихся инвалидов в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях

(наличие пандусов, поручней, расширенных дверных проемов, лифтов, при отсутствии лифтов аудитория располагается на первом этаже, наличие специальных кресел и других приспособлений).

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения для обучающихся с ограниченными возможностями здоровья и обучающихся инвалидов с разными видами ограничений здоровья:

- с нарушениями зрения:

Принтер Брайля braille embosser everest-dv4

Электронный ручной видеувелечитель САНЭД

- с нарушениями слуха:

средства беспроводной передачи звука (FM-системы);

акустический усилитель и колонки;

тифлофлешплееры, радиоклассы.

- с нарушениями опорно-двигательного аппарата:

передвижные, регулируемые эргономические парты с источником питания для индивидуальных технических средств;

компьютерная техника со специальным программным обеспечением;

альтернативные устройства ввода информации;

других технических средств приема-передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата.

Доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося инвалида или обучающегося с ограниченными возможностями здоровья обеспечен предоставлением ему не менее чем одного учебного, методического печатного и/или электронного издания по адаптационной дисциплине (включая электронные базы периодических изданий), в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для обучающихся с нарушениями зрения:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла;
- в печатной форме шрифтом Брайля.

Для обучающихся с нарушениями слуха:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Содержание адаптационной дисциплины размещено на сайте информационно-коммуникационной сети Интернет: Ссылка: <http://vlgr.ranepa.ru/sveden/education/> ...

Информационные средства обучения, адаптированные к ограничениям здоровья обучающихся:

электронные учебники, учебные фильмы по тематике дисциплины, презентации, интерактивные учебные и наглядные пособия, технические средства предъявления информации (мультимедийный комплекс) и контроля знаний (тестовые системы).

ЭБС «Айбукс», Информационно-правовые базы данных («Консультант Плюс», «Гарант»).

Мультимедийный комплекс в лекционной аудитории.

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

Волгоградский институт управления - филиал РАНХиГС
Экономический факультет
Кафедра информационных систем и математического моделирования

УТВЕРЖДЕНА
учёным советом
Волгоградского института управления –
филиала РАНХиГС
Протокол № 2 от 15.09.2022 г.

АДАптированная программа специалитета

"Экономико-правовое обеспечение экономической безопасности"

(наименование образовательной программы)

**Фонды оценочных средств промежуточной аттестации
по дисциплине**

**Б1.В.ДВ.09.02 Основы информационной безопасности
хозяйственной деятельности**

(код и наименование дисциплины)

38.05.01 Экономическая безопасность

(код, наименование направления подготовки /специальности)

Очная, заочная

(форма (формы) обучения)

Год набора – 2023 г.

Волгоград, 2022 г.

**Фонд оценочных средств промежуточной аттестации по дисциплине
Б1.В.ДВ.09.02 «Основы информационной безопасности хозяйственной деятельности»**

Промежуточная аттестация по дисциплине **Основы информационной безопасности хозяйственной деятельности** проводится в соответствии с Учебным планом для очной формы обучения: *в 3 семестре – в виде зачета.*

**Вопросы к зачету по дисциплине
«Основы информационной безопасности хозяйственной деятельности»**

1. Понятие защиты информации и информационной безопасности.
2. Основные составляющие информационной безопасности.
3. Законодательный уровень информационной безопасности.
4. Компьютерные преступления.
5. Понятие атаки на информационную систему.
6. Классификация атак.
7. Виды противников или “нарушителей”, их классификация.
8. Каналы утечки информации.
9. Понятие угрозы.
10. Источники угроз и их классификация.
11. Модель угроз.
12. Анализ возможных способов нарушений информационной системы.
13. Политика безопасности и ее реализация.
14. Основные понятия криптографии.
15. Два основных направления в современной криптографии.
16. Классические криптосистемы и их классификация. Примеры.
17. Криптоанализ многоалфавитных систем.
18. Криптосистема: “Одноразовый блокнот”.
19. Стандарты шифрования данных.
20. Системы шифрования, не требующие передачи ключа.
21. Криптография с открытым ключом.
22. Электронная подпись и принципы ее применения.
23. Руководящие документы Гостехкомиссии России.
24. Инструкция СТР-К. Рекомендации по защите конфиденциальной информации.
25. Разрешительная система допуска.
26. Межсетевые экраны.
27. Технология VPN-сетей.
28. Угрозы информационной безопасности при работе с Интернет.
29. Архитектура типовой системы защиты от несанкционированного доступа.
30. Идентификация и аутентификация. Парольная аутентификация.
31. Подсистема управления доступом. Матрица доступа и списки доступа.
32. Программно-аппаратные средства защиты информации от НСД.
33. Устройства ввода идентификационных признаков.
34. Комплексный подход к обеспечению информационной безопасности организации.
35. Перспективы развития технологий обеспечения информационной безопасности.

Практические задания к зачету

Тема 1. Защита офисных документов.

Рассматриваемые вопросы:

Защита документов Microsoft Word от несанкционированного доступа.

Защита документов Microsoft Word от несанкционированного изменения.

Защита документов Microsoft Excel от несанкционированного изменения.

Защита документов Microsoft Excel от несанкционированного доступа.

Задания для самостоятельного выполнения:

Защита документов Word.

1. Создайте на диске D: в папке вашей группы папку Защита офиса.

2. Наберите в редакторе Word произвольный текст и сохраните его в папке Защита офиса под именем document1.

3. Выберите меню Сервис – Установить защиту.

4. Запретите любые изменения кроме записи исправлений и задайте пароль 12345.

5. Попробуйте отредактировать свой текст. Удалите некоторые слова и допишите новые. Попробуйте принять все исправления (Сервис – Исправления – Принять/отклонить исправления). Обратите внимание, что все изменения в документе фиксируются, но принять/отклонить их невозможно.

6. Закройте документ, сохранив его.

7. Откройте документ и попробуйте принять исправления.

8. Снимите защиту документа. Выберите меню Сервис – Снять защиту и введите пароль.

9. Попробуйте принять все исправления. Убедитесь, что исправления приняты.

10. Заново защитите документ, кроме записи исправлений и закройте его, сохранив.

11. Наберите новый документ (отличный от первого) и сохраните его (под именем document2) в папке Защита офиса.

12. Установите защиту этого документа, выбрав меню Сервис – Установить защиту и запретив любые изменения кроме вставки примечаний. Задайте пароль 12345.

13. Попробуйте отредактировать документ.

14. Вставьте два примечания к любым фрагментам. Меню Вставка – Примечание.

15. Попробуйте изменить одно примечание и удалить другое.

16. Закройте документ, сохранив его.

17. Создайте третий документ в Word, сохраните его в папке Защита офиса под именем document3. Установите на него защиту, запретив любые изменения, кроме ввода данных в поля форм. Задайте пароль 12345.

18. Попробуйте отредактировать документ. Просмотрите пункты меню, чтобы выяснить Ваши возможности по редактированию документа.

19. Снимите защиту с документа.

20. Разбейте ваш документ на два раздела. (Установите курсор в место разрыва и выберите Меню Вставка – Разрыв – Новый раздел на текущей странице).

21. Установите защиту на документ, запретив любые изменения, кроме ввода данных в поля форм. Используя кнопку Разделы, установите запрет только на второй раздел. Пароль 12345.

22. Попробуйте отредактировать первый и второй разделы документа.

23. Закройте документ, сохранив его.

24. Создайте четвертый документ в редакторе Word и сохраните его в папке Защита офиса под именем document4.

25. Выберите меню Сервис – Параметры, затем вкладку Сохранение.

(Если Вы работаете в Word2t3 или XP, то надо выбрать вкладку Безопасность. Посмотрите возможности этой вкладки. Обратите внимание на флажок «Удалять личные сведения из файла при его сохранении»).

26. Задайте пароль 7777 на открытие файла.

27. Закройте файл, сохранив его, затем попробуйте открыть. Попробуйте ввести неправильный пароль, а затем откройте документ с правильным паролем.

28. Создайте пятый документ в редакторе Word и сохраните его в папке Защита офиса под именем document5.

29. Выберите меню Сервис – Параметры, затем вкладку Безопасность (Сохранение для Word2000) и задайте пароль разрешения записи 9999.

30. Закройте документ, сохранив его и попробуйте снова открыть. Выберите режим только чтения. Отредактируйте документ и попробуйте его сохранить. Сохраните как document5_1.

31. Попробуйте открыть файл document5_1.

32. Закройте все файлы и покажите результат преподавателю.

Защита документов Excel.

1. Запустите Excel и создайте следующую таблицу

ФИО	Оклад	Премия	Итого

2. Заполните ее для произвольных трех человек, вводя произвольные числа и суммируя их в графе Итого.

3. Постройте круговую диаграмму по столбцу Итого.

4. Сохраните файл в папке Защита офиса под именем proba1.

5. Сохраните этот же файл в папке Защита офиса еще раз под именем proba2.

6. Закройте файл proba2 и откройте файл proba1.

7. Выберите меню Сервис – Защита – Защитить лист и задайте пароль 1111.

8. Попробуйте отредактировать лист. Перейдите на Лист2 и попробуйте ввести данные.

9. Установите защиту второго листа с паролем 2222.

10. Снимите защиту с Листа1. Используйте меню Сервис – Защита – Снять защиту листа.

11. Установите защиту Листа1, отметив только флажок Защита листа в отношении объектов и задав пароль 1111.

12. Попробуйте изменить данные в ячейках. Попробуйте изменить диаграмму.

13. Закройте файл, сохранив его.

14. Откройте файл proba1 и попробуйте внести изменения на первый лист, затем на второй.

15. Закройте файл proba1 и откройте файл proba2.

16. Выберите меню Сервис – Защита – Защитить книгу. Оставьте отмеченным только флажок Структуру и задайте пароль kniga (проверьте, чтобы была включена английская раскладка)..

17. Попробуйте изменить данные на листе. Убедитесь, что изменения возможны.

18. Попробуйте удалить первый лист (пр. кнопка мыши на ярлыке листа внизу страницы).

19. Закройте файл, сохранив изменения, и заново откройте его (proba2).

20. Снимите защиту с книги. Меню Сервис – Защита – Снять защиту книги.

21. Установите защиту книги, отметив оба флажка и установив пароль kniga2.

22. Попробуйте изменить данные на листе.

23. Выберите меню Окно – Скрыть и введите пароль.

24. Закройте файл, сохранив изменения.

25. Откройте файл proba2. Убедитесь, что окно не отображается и данные не видны.

26. Выберите меню Окно – Отобразить и введите пароль.

27. Скройте окно и закройте файл, сохранив изменения.

28. Покажите результат преподавателю.

29. Снимите защиту со всех ваших файлов.

Литература:

www.microsoft.com

Лекционный материал.

Тема 2. Построение модели угроз.

Рассматриваемые вопросы:

Классификация атак.

Каналы утечки информации.

Понятие угрозы.

Источники угроз и их классификация.

Построение модели угроз.

Задания для самостоятельного выполнения:

Постройте модель угроз для некоторой организации, заполнив прилагаемую таблицу так, чтобы в ячейке стояла «1», если угроза, указанная в данной строке применима для объекта, указанного в данном столбце.

	Перечень источников угроз	Пути реализации	мониторы	Сист блоки	клавиатура	Принтеры	Копировально-множительные аппараты	магнитные носители инф-ции	Сеть электропитания	телефоны	Средства пожарной и охранной сигнализации
			1	2	3	4	5	6	7	8	9
Антропогенные источники угроз											
1	Интерес и преднамеренные действия криминальных структур и преступных группировок;	Утечка за счет агентов									
		Визуальная и фото разведка									
		Блокирование информации									
		Модификация информации									
		Уничтожение информации									
		Применение закладок									
2	Преднамеренные действия вспомогательного персонала (уборщики, охрана)	Утечка информации									
		Визуальная и фото разведка									
		Блокирование информации									
		Модификация информации									
		Уничтожение информации									
		Применение закладок									
3	Ошибки пользователей	Блокирование информации									
		Модификация информации									
		Уничтожение информации									
4	Ошибки программистов	Блокирование информации									
		Модификация информации									
		Уничтожение информации									
Техногенные источники угроз											
5	Сбои в каналах передачи и средствах связи;	Блокирование информации									
		Уничтожение информации									
6	Сбои в средствах электропитания	Блокирование информации									
		Уничтожение информации									
7	Возможность аварий в инженерных (водоснабжения, канализации) и коммуникационных сетях	Блокирование информации									
		Уничтожение информации									
Внешние стихийные источники											
8	Возможность ураганов	Уничтожение информации									
		Блокирование информации									
9	Возможность аварии близлежащих промышленных объектов	Уничтожение информации									
		Блокирование информации									
10	Возможность пожаров	Уничтожение информации									

Литература:

4. Лекционный материал.

5. Основы информационной безопасности хозяйственной деятельности: учебное пособие / И.П. Михнев; ВФ ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы». – Волгоград: Изд-во ВФ ФГБОУ ВПО РАНХиГС, 2013. – 144 с.

6. Платонов В. В. Программно-аппаратные средства защиты информации: учебник. / М.: Изд. центр "Академия". 2014.

Тема 3. Классические криптосистемы.

Рассматриваемые вопросы:

9. Классическая криптография.
10. Криптосистема Цезаря.
11. Криптосистема Виженера.
12. Практическая реализация системы Виженера.
13. Понятие многоалфавитной криптосистемы.
14. Криптоанализ многоалфавитной криптосистемы.
15. Криптоанализ системы Виженера.
16. Криптоанализ системы «Одноразовый блокнот».

Задания для самостоятельного выполнения:

1. Откройте файл CRYPTO1.XLS и посмотрите как реализована система Виженера.

2. Создайте в Excel следующую таблицу

Открытый текст					
Пароль					
Код букв текста					
Код букв пароля					
Сумма кодов букв					
Сумма по модулю					
Криптотекст					

3. Введите в первую строку произвольный текст по одной букве в каждую ячейку.

4. Введите во вторую строку таблицы произвольный пароль по одной букве в каждую ячейку. Если длина пароля меньше длины открытого текста, то начните набор пароля дальше, пока не закончится открытый текст.

5. Используя функцию КОДСИМВ, заполните четвертую и пятую строки таблицы для определения кодов каждой буквы открытого текста и пароля.

6. В пятой строке сложите третью и четвертую строки.

7. Если в пятой строке сумма превышает 255, то в шестой строке необходимо отнять 255 от числа в пятой строке. Используйте функцию ЕСЛИ.

8. В седьмой строке получите буквы зашифрованного текста, используя функцию СИМВОЛ.

9. Самостоятельно, используя описанные выше функции, расшифруйте полученный криптотекст. Для этого создайте ниже первой таблицы вторую таблицу.

10. Расшифруйте текст:

Ж С Я г з _ в Ц _ Ч Ц Ю б Х Ъ г _ Ц Ъ Я Ъ г ф г ж Ч Ш Я '

используя пароль «шифр». При наборе текста пропустите пробелы между буквами.

11. Расшифруйте текст:

Е Ы Я ж Ц С о _ Ъ в б У б д _ Щ ж _ У Ы з Ш Ф Ф _ Щ Щ а д _ Э п _ Э Э Ю б Э Р м н а к з
не зная пароля, но зная, что в зашифрованном тексте есть слово «истину».

Литература:

4. Лекционный материал.

5. Основы информационной безопасности хозяйственной деятельности: учебное пособие / И.П. Михнев; ВФ ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы». – Волгоград: Изд-во ВФ ФГБОУ ВПО РАНХиГС, 2013. – 144 с.

6. Платонов В. В. Программно-аппаратные средства защиты информации: учебник. / М.:

Тема 4. Криптография с открытым ключом.

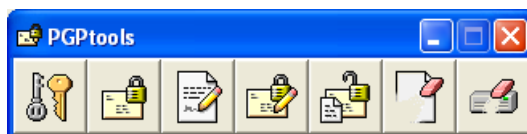
Рассматриваемые вопросы:

8. Криптография с открытым ключом.
9. Генерация ключевой пары в программе PGP.
10. Организация обмена ключами.
11. Шифрование данных в PGP.
12. Понятие электронной подписи.
13. Защита документов электронной подписью в программе PGP.
14. Шифрование и электронная подпись документов в PGP.


Задания для самостоятельного выполнения:

1. Запустите PGPtools (Пуск – Программы – PGP – PGPtools)


Появится панель




2. Выберите левую кнопку с двумя ключами. Запустится модуль PGPkeys со списком всех ключей на Вашем компьютере. В поле Description указано, какой это ключ: только открытый (public key) или ключевая пара, т.е. открытый и секретный ключ в комплекте (key pair).

3. Создайте новую ключевую пару, нажав на кнопку  и выполнив все шаги мастера создания ключей.

4. Создайте на диске D: папку с названием Вашей группы.


5. Экспортируйте свой открытый ключ в эту папку, нажав на кнопку  и указав путь до Вашей папки. В качестве названия файла с ключом укажите Вашу фамилию.

6. Скопируйте Ваш файл на сервер (Server606) в папку PublicKey.

7. Импортируйте из этой папки чьи-либо другие открытые ключи. Для этого нажмите на кнопку  и выберите путь и название файла.


8. Закройте окно PGPkeys.

9. Запустите Word и наберите письмо кому-либо, чей ключ вы импортировали. Сохраните этот текст в вашей папке.


10. Зашифруйте этот файл открытым ключом этого пользователя. Для этого нажмите кнопку  на панели PGPtools, укажите путь и название Вашего файла, а затем ключ в появившемся окне. Сохраните зашифрованный файл в Вашей папке под фамилией того, кому Вы писали.

11. Скопируйте этот файл на сервер (Server600) в папку TextPGP.

12. Скопируйте из этой папки в Вашу папку на диске D: файл, адресованный Вам.

13. Расшифруйте этот файл, нажав кнопку  или дважды щелкнув по нему мышкой, а затем выбрав Ваш ключ в списке ключей.

14. Создайте еще один документ в редакторе Word, сохранив его в Вашей папке на диске D:

15. Подпишите этот файл вашей электронной подписью. Для этого нажмите кнопку  на панели PGPtools, укажите путь и название Вашего файла, а затем Ваш ключ в появившемся окне.

16. Обратите внимание на файл подписи в вашей папке. Откройте его двойным щелчком.

17. Откройте подписанный Вами файл и измените его, сохранив изменения на диске.

18. Откройте файл подписи двойным щелчком еще раз. Убедитесь, что подпись не действительна.

19. Создайте новый документ в Word. Наберите небольшое предложение и скопируйте его в буфер обмена.

20. Щелкните мышкой по кнопке  на панели задач в правом нижнем углу.

21. В появившемся меню выберите Encrypt Clipboard и укажите Ваш ключ.

22. На чистом месте Вашего документа вставьте текст из буфера обмена (Правка – Вставить). Появился зашифрованный текст.

23. Скопируйте его в буфер обмена и по аналогии с шифрованием расшифруйте его, выбрав пункт Decrypt&Verify Clipboard.

24. Вставьте расшифрованный текст из буфера обмена.

Литература:

6. Лекционный материал.

7. Основы информационной безопасности хозяйственной деятельности: учебное пособие / И.П. Михнев; ВФ ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы». – Волгоград: Изд-во ВФ ФГБОУ ВПО РАНХиГС, 2013. – 144 с.

8. Платонов В. В. Программно-аппаратные средства защиты информации: учебник. / М.: Изд. центр "Академия". 2014.

9. Введение в криптографию/ Под общ. ред. В.В. Яценко. – М.: МЦНМО “ЧеРо”, 2013.

10. <http://pgp2all.org.ru>

Тема 5. Защита баз данных Microsoft Access.

Рассматриваемые вопросы:

6. Построение базы данных в Microsoft Access.
7. Защита базы данных от открытия.
8. Пользователи и группы.
9. Парольная защита.
10. Разграничение прав доступа.

Задания для самостоятельного выполнения:

1. Создайте на диске D: в папке вашей группы базу данных Секрет

2. Создайте таблицу в режиме конструктора (поле помеченное * является ключевым) и сохраните ее по имени Анкета.

	Имя поля	Тип данных
	Код	Счетчик
	ФИО	Текстовый
	Адрес	Текстовый
	Телефон	Текстовый

3. Введите в таблицу три записи.

4. Установите парольную защиту на эту базу данных (пароль 1234)

5. Создайте на диске D: в папке вашей группы базу данных Доступ.

6. Создайте для этой базы данных группы пользователей Student и Others

7. Создайте в группе Student пользователя под своей фамилией и пользователя Student1.

8. В группе Others создайте пользователя Friends и пользователя Guest.

9. Установите пароль администратору (admin) базы данных (**обязательно 7777**).

10. Установите пароли для созданных вами пользователей (пароли совпадают с именем пользователя).

11. Установите права доступа к базе данных для группы Student на все действия, кроме администрирования.

12. Установите права доступа к базе данных для группы Others только чтение и добавление данных.

13. Установите для группы Users права только на чтение данных и макета.

14. Покажите результат преподавателю.

15. Снимите пароль администратора

Литература:

3. Лекционный материал.
4. www.microsoft.com

Тема 6. Практическое применение межсетевых экранов.

Рассматриваемые вопросы:

4. Понятие межсетевого экрана.
5. Принципы работы с программой Firewall Outpost.
6. Настройка программных модулей.

Задания для самостоятельного выполнения:

Outpost Firewall

1. Загрузите программу Outpost Firewall.

2. Выберите пункт *Сетевая активность*. Окно справа содержит информацию о текущих соединениях приложений с сетью. Попробуйте получить информацию по какому-нибудь пункту.

3. Выберите пункт *Открытые порты*. Окно содержит информацию о том, какими процессами на компьютере открыты определенные порты.

4. Просмотрите пункты *Разрешенные* и *Заблокированные*, которые содержат общую статистику по соединениям.

5. Выберите пункт *DNS*. Кэширование запросов (т.е. сохранение ответов в базе Outpost) к DNS позволяет сократить время открытия страниц, которые были посещены ранее за счет того, что компьютеру не нужно будет перед открытием обращаться к DNS серверу для определения IP адреса открываемой страницы.

6. Просмотрите Журнал.

7. Щелкните правой кнопкой мыши по названию модуля DNS в левом окне программы и выберите *Параметры*.

8. Ограничьте кэш DNS на 50 записей и установите срок хранения 10 дней.

9. Выберите пункт *Детектор атак*, который хранит общую информацию о защите компьютера от атак, сканирования и других типов запрещенных соединений.

10. Просмотрите журнал. Щелкните правой кнопкой мыши по названию модуля *Детектор атак* в левом окне программы и выберите *Параметры*. В окне настроек при помощи ползунка можно выбрать один из трех уровней тревоги:

Максимальный – файрволл будет предупреждать о попытке подключения даже на один порт.

Обычный – предупреждение будет выдано только при сканировании с одного адреса нескольких портов или определенных портов, которые представляют определенный интерес.

Безразличный – файрволл будет сигнализировать лишь о реальной атаке на компьютер, а не о попытке исполнить такую атаку или просканировать порты.

11. Нажмите кнопку *Выбрать фильтр*. Просмотрите ее возможности.

12. Выберите пункт *Интерактивные элементы*. Здесь можно заблокировать всплывающие окна, переходы по рекламным сайтам в Интернет.

13. Просмотрите параметры настройки для данного пункта (правая кнопка мыши). На трех вкладках размещены настройки блокировки всех элементов, которые могут находиться на посещаемых веб-страницах или в почте. Большинство настроек имеют три настройки: *Разрешено*, *Запрос* и *Запрещено*. При настройке нужно учитывать тот факт, что на многих страницах скрипты или флэш могут использоваться для создания меню и если их полностью отключить, то навигация по сайту будет невозможна. Поэтому, оптимальным станет использование настройки *Запрос*. Для особой настройки некоторых сайтов в модуле *«Интерактивные элементы»* служит вкладка *«Исключения»*. С ее помощью можно сформировать список сайтов и настроить для каждого из них блокировку определенных элементов. Этот список имеет более высокий приоритет, чем общие настройки блокировки для всех сайтов.

14. Просмотрите вкладки параметров, запретите всплывающие окна и настройте остальное по своему усмотрению.

15. Выберите пункт *Реклама*. Outpost умеет отсекал рекламу по размеру и по содержимому ссылки, что экономит трафик и увеличивает скорость загрузки страниц.

16. Вызовите параметры для данного пункта (правая кнопка мыши). Установите флажок *Показать корзину для рекламы*. Если в стандартном списке отсутствует описание для определенного баннера, и он загружается при посещении страницы, то, открыв корзину, достаточно мышью перетащить в нее баннер, и он больше никогда не будет загружаться. Вкладка *Общие* позволяет выбрать то, чем будут заменяться вырезанные со страниц рекламные баннеры. Здесь же можно создать список сайтов, с которых не будет вырезаться графика и реклама.

17. Просмотрите все вкладки параметров.

18. Выберите пункт *Содержимое*. В настройках этого модуля можно задать список слов, которые могут встречаться на странице или в адресе страницы и которые будут служить Outpost–у сигналом того, что страницу отображать запрещено.

19. Просмотрите возможности данного пункта.

20. Выберите пункт *Фильтрация почтовых вложений*. В настройках этого модуля можно задать список типов файлов, которые подлежат переименованию, а так же включить вывод информационного сообщения о получении файлов определенного типа. Файл, тип которого указан в настройках этого модуля, при получении его почтовым клиентом, получит второе расширение «.safe». Это позволит избежать автоматического выполнения почтовым клиентом кода, что может являться причиной заражения компьютера вирусами.

21. Просмотрите параметры данного пункта и его возможности.

22. Доступ к общим настройкам программы можно получить при помощи пункта меню *Параметры – Общие* из главного меню программы или нажатием соответствующей кнопки на панели. Вызовите окно настройки параметров и просмотрите вкладку *Общие*.

23. Вкладка *«Приложения»* позволяет управлять правилами поведения файрволла при попытке доступа в сеть определенных приложений. На этой вкладке перечислены все приложения, которые обнаружены на компьютере Outpost–ом при установке. Сразу после инсталляции эти приложения находятся в группе *«Пользовательский уровень»*. Для них создано одно или несколько правил, указывающих, каким образом приложение может обмениваться данными с сетью. Правило можно просмотреть или изменить при помощи двойного клика по имени его исполняемого файла.

24. Просмотрите правила для некоторых приложений.

25. Приложения из группы *Запрещенные приложения* никогда не получают доступа в сеть, вся их сетевая активность будет пресечена файрволлом. Некоторым приложениям можно полностью открыть доступ в сеть, переместив их в группу *«Доверенные приложения»*. Их доступ в сеть не ограничивается ничем, никакими правилами. Перемещение приложений из групп в группу, равно как и изменение правил, созданных для приложений, выполняется при помощи кнопки *Изменить*. При помощи кнопки *Добавить* можно внести в список новое приложение и затем создать для него правило общения с сетью.

26. Переместите приложение Excel в группу *Запрещенные приложения*.

27. Просмотрите оставшиеся вкладки настроек программы.

28. Попробуйте через сетевое окружение выйти на компьютер соседа.

29. Проверьте реакцию файрвола на попытку соседа обратиться к вашему компьютеру.

30. Перейдите в настройки общих параметров программы.

31. Выберите вкладку *Системные*. Уберите флажок NetBIOS. Теперь ваш компьютер недоступен по сети.

32. Дождитесь, когда ваш сосед выполнит предыдущее задание и попробуйте через сетевое окружение обратиться к его компьютеру.

33. Включите флажок NetBIOS на своем компьютере.

34. Вызовите журнал, нажав соответствующую кнопку на панели инструментов.

35. Просмотрите журнал.

Литература:

5. Лекционный материал.

6. Документация по работе с программой Firewall Outpost.

7. Основы информационной безопасности хозяйственной деятельности: учебное пособие / И.П. Михнев; ВФ ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы». – Волгоград: Изд-во ВФ ФГБОУ ВПО РАНХиГС, 2013. – 144 с.

8. Платонов В. В. Программно-аппаратные средства защиты информации: учебник. / М.: Изд. центр "Академия". 2014.

Тема 7. Защита информации в Интернет.

Рассматриваемые вопросы:

4. Принципы работы межсетевых экранов при работе с Интернет.
5. Настройка программных модулей при работе с Интернет.
6. Блокирование ненужного трафика и рекламы.

Задания для самостоятельного выполнения:

1. Загрузите программу Outpost Firewall.
2. Откройте в Internet Explorer страницу www.yandex.ru
3. Выберите пункт *Сетевая активность*. Просмотрите информацию о текущих соединениях с сетью.
4. Выберите пункт *Открытые порты*. Получите информацию о том, какими процессами на компьютере открыты определенные порты.
5. Просмотрите пункты *Разрешенные* и *Заблокированные*, которые содержат общую статистику по соединениям.
6. Выберите пункт DNS и в параметрах ограничьте кэш DNS на 50 записей и установите срок хранения 10 дней.
7. Выберите пункт *Детектор атак* и в параметрах задайте *Обычный* уровень тревоги.
8. Выберите пункт *Интерактивные элементы*. Просмотрите параметры настройки для данного пункта. На трех вкладках размещены настройки блокировки всех элементов, которые могут находиться на посещаемых веб-страницах или в почте. Настройте параметры по своему усмотрению (рекомендуется чаще использовать настройку *Запрос*).
9. Откройте в Internet Explorer страницу www.mail.ru, перейдите по какой-нибудь ссылке новостей.
10. Просмотрите в Outpost Firewall статистику по соединениям, а также статистику детектора атак.
11. Выберите пункт *Реклама*. Вызовите параметры для данного пункта. Установите флажок *Показать корзину для рекламы*.
12. Откройте стартовую страницу www.mail.ru и мышью перетащите в *Корзину для рекламы* рекламные баннеры с этой страницы.
13. Закройте страницу и попробуйте заново ее открыть. Проверьте, что происходит с рекламными баннерами.
14. Просмотрите все оставшиеся вкладки параметров.
15. Выберите пункт *Содержимое*. В настройках этого модуля можно задать список слов, которые могут встречаться на странице или в адресе страницы и которые будут служить Outpost–у сигналом того, что страницу отображать запрещено.
16. Настройте программу так, чтобы Outpost блокировал все страницы, в адресе которых присутствует слово chat. Попробуйте открыть страницу www.chat.ru.
17. Выберите пункт *Фильтрация почтовых вложений*. В настройках этого модуля можно задать список типов файлов, которые подлежат переименованию, а так же включить вывод информационного сообщения о получении файлов определенного типа.
18. Задайте вывод информационного сообщения для всех файлов с расширением .zip и переименование файлов с расширением .exe.
19. Покажите результат преподавателю.
20. Отмените все свои настройки и закройте все открытые приложения.

Литература:

4. Лекционный материал.
5. Основы информационной безопасности хозяйственной деятельности: учебное посо-

бие / И.П. Михнев; ВФ ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы». – Волгоград: Изд-во ВФ ФГБОУ ВПО РАНХиГС, 2013. – 144 с.

6. Платонов В. В. Программно-аппаратные средства защиты информации: учебник. / М.: Изд. центр "Академия". 2014.

Тема 8. Типовая структура защиты от НСД. Управление доступом.

Рассматриваемые вопросы:

5. Типовая структура защиты информации от НСД.
6. Подсистема управления доступом.
7. Построение матрицы доступа.
8. Документация отдела обеспечения информационной безопасности.

Задания для самостоятельного выполнения:

1. Рассмотрите типовую структуру защиты информации от НСД.
2. Продумайте структуру защиты информации от НСД для произвольной (вымышленной) организации.
3. Рассмотрите подсистему управления доступом для этой организации.
4. Составьте перечень защищаемых информационных ресурсов организации.
5. Постройте матрицу доступа для данной организации.
6. Составьте документ, определяющий правила доступа пользователей к ресурсам при помощи личных идентификаторов и паролей, правила составления, смены и хранения паролей.
7. Сохраните все документы в своей личной папке (и на своей дискете).

Литература:

3. Лекционный материал.
4. Основы информационной безопасности хозяйственной деятельности: учебное пособие / И.П. Михнев; ВФ ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы». – Волгоград: Изд-во ВФ ФГБОУ ВПО РАНХиГС, 2013. – 144 с.

ИТОГОВЫЙ ТЕСТ ПО КУРСУ

«Основы информационной безопасности хозяйственной деятельности»

Электронный тест представляет собой задания с выбором только одного правильного ответа из предложенных. Результат программа Unitest выводит в процентах.

1. Криптография это

- А) наука о методах преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для несанкционированных лиц
- В) наука о методах и способах раскрытия шифров
- С) совокупность методов, скрывающих факт передачи секретной информации за открытой информацией
- Д) совокупность методов, обеспечивающих абсолютную надежность канала передачи данных от перехвата
- Е) наука о методах создания цифровой подписи

2. Какая из следующих криптоаналитических атак считается наиболее опасной?

- А) при наличии только одного зашифрованного фрагмента
- В) при наличии большого набора зашифрованных фрагментов
- С) при наличии фрагмента открытого текста и соответствующего ему криптотекста
- Д) при известном методе шифрования
- Е) при возможности выбора любого открытого текста и получении соответствующего ему криптотекста

3. Сколько различных ключей в системе Цезаря при использовании полного русского алфавита?

- A) 16
- B) 33
- C) 66
- D) 256
- E) 1024

4. Что является ключом в криптосистеме Виженера?

- A) любое дробное число
- B) величина сдвига исходного алфавита
- C) переставленный алфавит
- D) случайная последовательность букв, равная длине сообщения
- E) любое слово

5. Какая из перечисленных криптосистем является системой с открытым ключом?

- A) DES
- B) RSA
- C) Энигма
- D) ГОСТ 28147
- E) Цезаря

6. Можно ли в программе PGP воспользоваться чужим открытым ключом для расшифровки информации.

- A) да
- B) нет
- C) да, если известен тот пароль
- D) да, если пользователь даст права на расшифровку его информации и сообщит свой пароль
- E) да, если перебрать все ключи

7. Как раскрываются криптосистемы одноалфавитной замены?

- A) такие системы раскрыть нельзя
- B) полный перебор ключей
- C) анализ частот встречаемых букв
- D) перебор сообщений
- E) перестановки букв криптотекста

8. Криптоанализ это

- A) наука о методах преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для несанкционированных лиц
- B) наука о методах и способах раскрытия шифров
- C) совокупность методов, скрывающих факт передачи секретной информации за открытой информацией
- D) совокупность методов, обеспечивающих абсолютную надежность канала передачи данных от перехвата
- E) наука о методах создания цифровой подписи

9. Что является ключом в криптосистеме Цезаря?

- A) любое слово
- B) любое число
- C) величина сдвига исходного алфавита
- D) переставленный алфавит
- E) случайная последовательность символов

10. Какова длина ключа в стандарте шифрования ГОСТ 28147?

- A) 256 бит
- B) 64 бит
- C) 56 бит
- D) 1024 бит
- E) 2048 бит

11. На сложности решения какой математической задачи основана система RSA?

- A) коды исправляющие ошибки
- B) дискретный логарифм
- C) задача “о рюкзаке”
- D) разложение больших чисел на простые множители
- E) сложение по модулю два

12. Криптографический протокол это

- A) метод шифрования данных
- B) метод криптоанализа данных
- C) метод перехвата данных
- D) алгоритм обмена информацией между различными участниками при секретной передаче данных
- E) особая криптосистема

13. Криптосистема «Одноразовый блокнот» это:

- A) перестановочная система
- B) одноалфавитная система простой замены
- C) многоалфавитная система
- D) система с открытым ключом
- E) такой системы не существует

14. Какой пароль наиболее надежен?

- A) Фамилия пользователя
- B) Фраза из книги
- C) случайная последовательность цифр
- D) случайная последовательность букв
- E) случайная последовательность произвольных символов

15. Какова длина ключа в системе шифрования DES?

- A) 256 бит
- B) 64 бит
- C) 2048 бит
- D) 1024 бит
- E) 512 бит

16. Криптотекст это

- A) текст исходного сообщения
- B) текст зашифрованного сообщения
- C) пароль
- D) текст, полученный при криптоанализе
- E) ключ

17. Тайнопись (стеганография) это

- A) наука о методах преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для несанкционированных лиц
- B) наука о методах и способах раскрытия шифров
- C) совокупность методов, скрывающих факт передачи секретной информации за открытой информацией
- D) совокупность методов, обеспечивающих абсолютную надежность канала передачи данных от перехвата
- E) наука о методах создания цифровой подписи

18. Что позволяет определить метод Казиски при криптоанализе системы Виженера?

- A) пароль

- В) открытый текст
- С) метод шифрования
- Д) длину пароля
- Е) длину открытого текста

19. Какая криптосистема обеспечивает абсолютную надежность защиты при правильном ее использовании?

- А) DES
- В) RSA
- С) ГОСТ 28147
- Д) Одноразовый блокнот
- Е) Виженера

20. Обеспечивает ли пароль на вход в Windows надежную защиту компьютера?

- А) да
- В) нет
- С) при длине пароля более 10 символов
- Д) при случайном пароле
- Е) при регулярной смене пароля

21. Можно ли в программе PGP воспользоваться чужим открытым ключом для расшифровки информации.

- А) да
- В) нет
- С) да, если известен тот пароль
- Д) да, если пользователь даст права на расшифровку его информации и сообщит свой пароль
- Е) да, если перебрать все ключи

22. Как раскрываются криптосистемы одноалфавитной замены?

- А) такие системы раскрыть нельзя
- В) полный перебор ключей
- С) анализ частот встречаемых букв
- Д) перебор сообщений
- Е) перестановки букв криптотекста

23. Криптоанализ это

- А) наука о методах преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для несанкционированных лиц
- В) наука о методах и способах раскрытия шифров
- С) совокупность методов, скрывающих факт передачи секретной информации за открытой информацией
- Д) совокупность методов, обеспечивающих абсолютную надежность канала передачи данных от перехвата
- Е) наука о методах создания цифровой подписи

24. Что является ключом в криптосистеме Цезаря?

- А) любое слово
- В) любое число
- С) величина сдвига исходного алфавита
- Д) переставленный алфавит
- Е) случайная последовательность символов

25. Какова длина ключа в стандарте шифрования ГОСТ 28147?

- А) 256 бит
- В) 64 бит
- С) 56 бит
- Д) 1024 бит
- Е) 2048 бит

26. На сложности решения какой математической задачи основана система RSA?

- A) коды исправляющие ошибки
- B) дискретный логарифм
- C) задача “о рюкзаке”
- D) разложение больших чисел на простые множители
- E) сложение по модулю два

27. Криптографический протокол это

- A) метод шифрования данных
- B) метод криптоанализа данных
- C) метод перехвата данных
- D) алгоритм обмена информацией между различными участниками при секретной передаче данных
- E) особая криптосистема

27. Криптосистема «Одноразовый блокнот» это:

- A) перестановочная система
- B) одноалфавитная система простой замены
- C) многоалфавитная система
- D) система с открытым ключом
- E) такой системы не существует

29. Какой пароль наиболее надежен?

- A) Фамилия пользователя
- B) Фраза из книги
- C) случайная последовательность цифр
- D) случайная последовательность букв
- E) случайная последовательность произвольных символов

30. Какова длина ключа в системе шифрования DES?

- A) 256 бит
- B) 64 бит
- C) 2048 бит
- D) 1024 бит
- E) 512 бит