Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Баламирзоев Назим Лиодинович
Должность: Врио ректора
Дата подписания: 03.06.2022 13:13:09
Уникальный программный ключ:
777029a1882856141bfb9e855f0a3c8b6edae59e

Министерство науки и высшего образования и Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

РЕКОМЕНДОВАНО К УТВЕРЖДЕНИЮ:

Директор филиала ДГТУ
в г. Дербенте И. М. Мейланов,
_____:
Подпись
20.08 2018 г.

УТВЕРЖДАЮ:

Проректор по учебной работе
Суракатов Н. С.
Подпись ИОФ
21.08. 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Б1.В.ДВ.3 Защита информации
наименование дисциплины по ООП и код по ФГОС

для направления 38.03.01 – «Экономика»
шифр и полное наименование направления

по профилю «Экономика предприятий и организаций»
шифр и полное наименование профиля

Факультет: Филиал в городе Дербенте, Кафедра ЕГОиСД
наименование факультета, кафедра, где ведется дисциплина

Квалификация выпускника (степень): бакалавр
бакалавр

Форма обучения очная, курс 1, семестр(ы) 2
очная, заочная, др.

Всего трудоемкость в зачетных единицах (часах) 2 ЗЕТ (72ч.)

лекции 17 (час) экзамен _____
(семестр)

практические (семинарские) занятия ____ (час); зачет 2
(семестр)

лабораторные занятия 17 (час); самостоятельная работа 38 (час);

курсовой проект (работа, РГР) _____ (семестр).

Зав. кафедрой ЕГО и СД _____ Г.М. Гусейнова
подпись

Начальник УО _____ Э.В. Магомаева
подпись

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций примерной ООП ВО по направлению 38.03.01 «Экономика» и по профилю «Экономика предприятий и организаций».

Программа одобрена на заседании выпускающей кафедры
от 06.09.2018 года, протокол № 1.

Зав. выпускающей кафедрой по данному профилю

подпись — Г.М. Гусейнова (И.О.Ф)

ОДОБРЕНО
Методическим советом филиала
38.00.00
шифр и полное наименование

Экономика
направления

Председатель к.ф.н.,Г.М.Гусейнова
подпись, ИОФ

12.09. 2018г.

АВТОР ПРОГРАММЫ
Джумалиева Е.Р..
подпись, ИОФ

ст.преподаватель
ФИО, уч.степень, ученое звание, подпись

1. Цели дисциплины

Целями изучения дисциплины являются:

- понимание моделей и стандартов информационной безопасности;
- усвоение методов защиты информационных систем;
- приобретение теоретических знаний и практических навыков по использованию современных программных средств для обеспечения информационной безопасности и защиты информации от несанкционированного использования.
- формирование у студентов мотивации к самообразованию за счет активизации самостоятельной познавательной деятельности.

Задачами для достижения поставленных целей являются:

- изучение и классификация причин нарушений безопасности;
- проектирование мониторов безопасности субъектов и объектов;
- приобретение практических навыков работы с современными сетевыми фильтрами и средствами криптографического преобразования информации

2.Место дисциплины в структуре ООП

Дисциплина «Защита информации» является дисциплиной по выбору вариативной части дисциплин Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению 38.03.01 «Экономика».

Дисциплина преподается параллельно с изучением «Информатики», а после ее освоения на четвертом курсе студенты углубят полученные знания при изучении дисциплины «Профессиональные компьютерные программы».

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

- способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-1);
- способностью осуществлять сбор, анализ и обработку данных, необходимых для решения профессиональных задач (ОПК-2);
- способностью выбрать инструментальные средства для обработки экономических данных в соответствии с поставленной задачей, проанализировать результаты расчетов и обосновать полученные выводы (ОПК-3);
- способностью использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии (ПК-8);

Требования к результатам освоения дисциплины

В результате освоения дисциплины «Защита информации» студент должен:

знать:

- основные понятия и определения, используемые при изучении информационной безопасности;
- классификацию угроз информационной безопасности;
- классические и современные методы взлома интрасетей;
- классификацию "компьютерных вирусов", какую угрозу они представляют для безопасности информации и правила защиты от "компьютерных вирусов";
- как организовать информационную безопасность на предприятии
- нормы и требования российского законодательства в области лицензирования и сертификации;
- структуру коммерческой тайны предприятия

уметь:

- правильно выбрать и использовать антивирусную программу;
- восстанавливать пораженные "компьютерными вирусами" объекты;
- подключить организацию к Internet с соблюдением требований информационной безопасности;
- выявлять и классифицировать угрозы информационной безопасности предприятия
- планировать мероприятия по защите информации, исходя из известных угроз и финансовых возможностей предприятия

владеть:

–навыками самостоятельной работы с персональным компьютером как офисной системой в повседневной деятельности для подготовки документов и обмена информацией;
–основными методами, способами и средствами получения, хранения, переработки информации;
–методикой построения стандартных теоретических и эконометрических моделей для анализа и содержательной интерпретации полученных результатов;
-методами организации раздельного доступа к файлам и папкам на компьютере

4.Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетные единицы (72 часа). 17 лк, 17 лб, 38 срс. Форма промежуточной аттестации – зачет.2 семестр

4.1 Содержание дисциплины.

№ п/п	Наименование блока (раздела)	Наименование тем блока (раздела) дисциплины	семестр	неделя	Лекции	Лабораторная работа	СРС	Формы текущего * контроля успеваемости (по срокам текущих
1.	Актуальность информационной безопасности в современных условиях.	Международные стандарты информационного обмена. Получение статистических знаний об атаках, которым подвергаются компьютерные системы и потерях банков. Изучение основных понятий и определений, используемых при изучении дисциплины	2	1-2	2	2	5	Входной контроль
2	Понятие угрозы	Понятие угрозы. Получение знаний о видах угроз, путей и каналов утечки информации, от кого они исходят и к чему приводят. Изучение видов атак и методов взлома интрасетей злоумышленниками. Три вида возможных нарушений информационной системы. Виды противников или «нарушителей». Информационная безопасность в условиях функционирования в России глобальных сетей	2	3-4	2	2	5	
3	Понятия о видах вирусов	Получение знаний о существующих "компьютерных вирусах". Классификация "компьютерных вирусов". Угроза вирусов безопасности информации. Алгоритмы работы "компьютерных вирусов" и пути их внедрения в систему. Индивидуальные признаки, используемые для определения "компьютерных вирусов" различных классов.	2	5-6	2	2	5	Аттестационная контрольная работа1
4	Современные методы защиты информации	Ограничение доступа, разграничение доступа, разделение доступа, криптографическое преобразование информации, контроль и учет доступа, законодательные меры, обеспечение информационной безопасности в Internet. Основные технологии построения защищенных ИС. Место информационной безопасности в национальной безопасности страны. Концепция информационной безопасности.	2	7-8	2	2	5	
5	Информ	Сетевые модели передачи данных.	2	9-	2	2	5	Аттестационна

	ационная безопасность вычислительных сетей	Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика. Принципы защиты распределенных вычислительных сетей.		10				я контрольная работа2
6	Модели безопасности и их применение	Дискреционная и мандатная модели политики безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем	2	11-12	2	2	5	
7	Методы криптографии	Традиционные и современные криптосистемы. Методы шифрования данных. Основные криптографические алгоритмы. Абонентское и пакетное шифрование. Взаимное подтверждение подлинности (аутентификация) абонентов и объектов сети. Обеспечение целостности информации на основе электронной цифровой подписи.	2	13-14	2	2	5	Аттестационная контрольная работа 3
8	Лицензирование и сертификация в ИБ	Нормы и требования российского законодательства в области лицензирования и сертификации. Правила построения и функционирования системы лицензирования ФАПСИ. Порядок оформления и получения лицензий и сертификатов в области информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	2	15-17	3	3	3	
	всего		**2**	**17**	**17**	**17**	**38**	**зачет**

4.2Тематика лабораторных занятий (с указанием наименования и количества часов)

№ лабор. работы	Наименование лабораторной работы	Количество часов
1	Политика безопасности предприятия	2
2	Назначение паролей и логинов	2
3	Проверка в системе аутентификации	2
4	Симметричное кодирование	2
5	Асимметричное кодирование	2
6	Электронно – цифровая подпись	4

7	Восстановление данных	3
	ИТОГО:	17

4.3 Тематика для самостоятельной работы студентов

Общее количество 38 часов.

1 Концепция информационной безопасности
2. Политики безопасности в компьютерных сетях
3. Угрозы информационной безопасности в компьютерных системах
4. Защита информации от несанкционированного доступа.
5. Криптографические методы защиты информации
6. Технологии межсетевых экранов
7. Технологии виртуальных защищенных сетей VPN
8. Безопасность сетевых протоколов уровней модели OSI
9. Вирусы как угроза ИБ
10.Средства антивирусной защиты

Структура и содержание дисциплины «Защита информации» для заочной формы обучения Общая трудоемкость дисциплины составляет 2 зачетные единицы (72 часа). 4 лк, 4 лб, срс.-60 Форма отчетности – зачет 1 курс

4.4 Содержание дисциплины.

№ п/п	Наименование блока (раздела)	Наименование тем блока (раздела) дисциплины	курс	Лекции	Лабораторная работа	СРС	Формы текущего * контроля успеваемости (по срокам текущих
1.	Актуальность информационной безопасности в современных условиях.	Международные стандарты информационного обмена. Получение статистических знаний об атаках, которым подвергаются компьютерные системы и потерях банков. Изучение основных понятий и определений, используемых при изучении дисциплины	1	2	2	8	
2	Понятие угрозы	Понятие угрозы. Получение знаний о видах угроз, путей и каналов утечки информации, от кого они исходят и к чему приводят. Изучение видов атак и методов взлома интрасетей злоумышленниками. Три вида возможных нарушений информационной системы. Виды противников или «нарушителей». Информационная безопасность в условиях функционирования в России глобальных сетей	1	2	2	8	
3	Понятия о видах вирусов	Получение знаний о существующих "компьютерных вирусах". Классификация "компьютерных вирусов". Угроза вирусов	1			6	

		безопасности информации. Алгоритмы работы "компьютерных вирусов" и пути их внедрения в систему. Индивидуальные признаки, используемые для определения "компьютерных вирусов" различных классов.					
4	Современные методы защиты информации	Ограничение доступа, разграничение доступа, разделение доступа, криптографическое преобразование информации, контроль и учет доступа, законодательные меры, обеспечение информационной безопасности в Internet. Основные технологии построения защищенных ИС. Место информационной 1безопасности в национальной безопасности страны. Концепция информационной безопасности.	1			6	
5	Информационная безопасность вычислительных сетей	Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика. Принципы защиты распределенных вычислительных сетей.	1			8	
6	Модели безопасности и их применение	Дискреционная и мандатная модели политики безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем	1			6	
7	Методы криптографии	Традиционные и современные криптосистемы. Методы шифрования данных. Основные криптографические алгоритмы. Абонентское и пакетное шифрование. Взаимное подтверждение подлинности (аутентификация) абонентов и объектов сети. Обеспечение целостности информации на основе электронной цифровой подписи.	1			8	
8	Лицензирование и сертификация в ИБ	Нормы и требования российского законодательства в области лицензирования и сертификации. Правила построения и функционирования системы лицензирования ФАПСИ. Порядок оформления и получения лицензий и	1			10	

		сертификатов в области информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы					
	всего		**1**	**4**	**4**	**60**	**зачет**

4.5 Тематика лабораторных занятий (с указанием наименования и количества часов)

№ лабор. работы	Наименование лабораторной работы	Количество часов
1	Политика безопасности предприятия	2
2	Назначение паролей и логинов	2
3	Проверка в системе аутентификации	
4	Симметричное кодирование	
5	Асимметричное кодирование	
6	Электронно – цифровая подпись	
7	Восстановление данных	
	ИТОГО:	**4**

4.6 Тематика для самостоятельной работы студентов

Общее количество 60 часов.

1 Концепция информационной безопасности

2. Политики безопасности в компьютерных сетях

3. Угрозы информационной безопасности в компьютерных системах

4. Защита информации от несанкционированного доступа.

5. Криптографические методы защиты информации

6. Технологии межсетевых экранов

7. Технологии виртуальных защищенных сетей VPN

8. Безопасность сетевых протоколов уровней модели OSI

9. Вирусы как угроза ИБ

10.Средства антивирусной защиты

5. Образовательные технологии

При изучении дисциплины предусматривается использование в учебном процессе активных интерактивных форм проведения занятий в объеме 20% от аудиторной нагрузки.

Теоретическая часть курса реализуется в основном на лекциях и в ходе самостоятельной работы студентов, а практическая часть – на практических занятиях формы, проведения которых могут быть весьма разнообразны: наряду с традиционными занятиями проводятся деловые игры, разрабатываются исследовательские проекты, проводится работа в команде,используются методы проблемного обучения, ведется опережающая самостоятельная работа. В процессе изучения дисциплины используются как традиционные, так и инновационные технологии, активные и интерактивные методы и формы обучения: практические занятия, проектный метод, поисковый метод исследовательский метод, мозговой штурм, разбор конкретных ситуаций, творческие задания для самостоятельной работы, информационные технологии.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно2-методическое обеспечение самостоятельной работы студентов

Тесты входного контроля

Как называется умышленно искаженная информация?

+ Дезинформация

- Информативный поток
- Достоверная информация
- Перестает быть информацией

Как называется информация, к которой ограничен доступ?

+ Конфиденциальная
- Противозаконная
- Открытая
- Недоступная

Какими путями может быть получена информация?

+ проведением, покупкой и противоправным добыванием информации научных исследований
- захватом и взломом ПК информации научных исследований
- добыванием информации из внешних источников и скремблированием информации научных исследовании
- захватом и взломом защитной системы для информации научных исследований

Как называются компьютерные системы, в которых обеспечивается безопасность информации?

+ защищенные КС
- небезопасные КС
- Само достаточные КС
- Саморегулирующиеся КС

Основной документ, на основе которого проводится политика информационной безопасности?

+ программа информационной безопасности
- регламент информационной безопасности
- политическая информационная безопасность
- Протекторат

В зависимости от формы представления информация может быть разделена на?

+ Речевую, документированную и телекоммуникационную
- Мысль, слово и речь
- цифровая, звуковая и тайная
- цифровая, звуковая

К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации

+ Информационным процессам
- Мыслительным процессам
- Машинным процессам
- Микропроцессам

Что называют защитой информации?

+ Все ответы верны
- Называют деятельность по предотвращению утечки защищаемой информации
- Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
- Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию

Под непреднамеренным воздействием на защищаемую информацию понимают?

+ Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию
- Не ограничения доступа в отдельные отрасли экономики или на конкретные производства

Шифрование информации это

+ Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
- Процесс преобразования, при котором информация удаляется
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Процесс преобразования информации в машинный код

Основные предметные направления Защиты Информации?
+ охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности
- Охрана золотого фонда страны
- Определение ценности информации
- Усовершенствование скорости передачи информации

Государственная тайна это
+ защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
- ограничения доступа в отдельные отрасли экономики или на конкретные производства
- защищаемые банками и иными кредитными организациями сведения о банковских операциях
- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

Коммерческая тайна это….
- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
+ ограничения доступа в отдельные отрасли экономики или на конкретные производства
- защищаемые банками и иными кредитными организациями сведения о банковских операциях
- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

Банковская тайна это….
- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
- ограничения доступа в отдельные отрасли экономики или на конкретные производства
+ защищаемые банками и иными кредитными организациями сведения о банковских операциях
- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

Профессиональная тайна
- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
- ограничения доступа в отдельные отрасли экономики или на конкретные производства
- защищаемые банками и иными кредитными организациями сведения о банковских операциях
+ защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

К основным объектам банковской тайны относятся следующие:
+ Все ответы верны
- Тайна банковского счета
- Тайна операций по банковскому счету
- Тайна банковского вклада

Как называется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений?
+ Тайна связи
- Нотариальная тайна
- Адвокатская тайна
- Тайна страхования

Как называются сведения, доверенные нотариусу в связи с совершением нотариальных действий?
+ Нотариальная тайна
- Общедоступные сведения
- Нотариальный секрет
- Нотариальное вето

Элемент аппаратной защиты, где используется установка источников бесперебойного питания (UPS)?

+ защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право

- управление доступом
+ конфиденциальность
- аутентичность
- целостность
- доступность

Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем

- защита от сбоев в электропитании
+ защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
+ защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
+ защита от утечек информации электромагнитных излучений

Какая из перечисленных атак на поток информации является пассивной:

+ перехват.
- имитация.
- модификация.
- фальсификация.
- прерывание.

К открытым источникам информация относятся.

+ Газеты, Радио, Новости
- Информация украденная у спецслужб
- Из вскрытого сейфа
- Украденная из правительственной организации

Технические каналы утечки информации делятся на…

+ Все перечисленное
- Акустические и виброакустические
- Электрические
- Оптические

Какой технический канал утечки отвечает за распространение звуковых колебаний в любом звукопроводящем материале или среде?

+ Акустические и виброакустические
- Электрические
- Оптические
- Радиоканалы

Какой технический канал утечки отвечает за напряжение и токи в различных токопроводящих коммуникациях?

- Акустические и виброакустические
+ Электрические

- Оптические
- Радиоканалы

Какой технический канал утечки отвечает за электромагнитные излучения радиодиапазона?

- Акустические и виброакустические
- Электрические
- Оптические
+ Радиоканалы

Какой технический канал утечки отвечает за электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра?

- Акустические и виброакустические
- Электрические
+ Оптические
- Радиоканалы

По сведениям Media и Pricewaterhouse Coopers, на чью долю приходится 60% всех инцидентов IT-безопасности?

- Хакерские атаки
- Различные незаконные проникновения
+ Инсайдеры
- Технические компании

Учет всех возможных коммуникационных каналов, обеспечения физической безопасности, шифрования резервных копий и информации, покидающей корпоративный периметр, и других организационных мероприятий это?

- Индивидуальный подход к защите
+ Комплексный подход к защите
- Смешанный подход к защите
- Рациональный подход к защите

Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе

+ Информационная безопасность
- Защитные технологии
- Заземление
- Конфиденциальность

Можно выделить следующие направления мер информационной безопасности

- Правовые
- Организационные
+ Все ответы верны
- Технические

Что можно отнести к правовым мерам ИБ?

+ Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
- охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра итд
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое
- охрану вычислительного центра, установку сигнализации и многое другое

Что можно отнести к организационным мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.

+ Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем.
- Охрану работоспособности отдельных звеньев и организацию вычислительных сетей с возможностью перераспределения ресурсов.
- Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

Что можно отнести к техническим мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
- Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
+ Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое
- Простые и доступные меры защиты от хищений, саботажа, диверсий, взрывов
- В административных местах установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

Потенциальные угрозы, против которых направлены технические меры защиты информации

+ Потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей
- Потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения
- Потери информации из-за не достаточной установки резервных систем электропитании и оснащение помещений замками.
- Потери информации из-за не достаточной установки сигнализации в помещении.
- Процессы преобразования, при котором информация удаляется

Шифрование информации это

+ Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
- Процесс преобразования, при котором информация удаляется
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Процесс преобразования информации в машинный код

Какие сбои оборудования бывают?

+ сбои работы серверов, рабочих станций, сетевых карт и тд
- потери при заражении системы компьютерными вирусами
- несанкционированное копирование, уничтожение или подделка информации
- ознакомление с конфиденциальной информацией

Какие сбои оборудования, при которых теряется информация, бывают?

- случайное уничтожение или изменение данных
+ перебои электропитания
- некорректное использование программного и аппаратного обеспечения, ведущее к уничтожению или изменению данных
- несанкционированное копирование, уничтожение или подделка информации

Какие потери информации бывают из-за некорректной работы программ?

- сбои работы серверов, рабочих станций, сетевых карт и тд
- перебои электропитания
+ потеря или изменение данных при ошибках ПО
- ознакомление с конфиденциальной информацией

Какие потери информации бывают из-за некорректной работы программ?

+ потери при заражении системы компьютерными вирусами
- сбои дисковых систем
- перебои электропитания
- сбои работы серверов, рабочих станций, сетевых карт и тд

Какие потери информации, связанные с несанкционированным доступом, бывают?

+ несанкционированное копирование, уничтожение или подделка информации
- потери при заражении системы компьютерными вирусами
- случайное уничтожение или изменение данных
- сбои дисковых систем

Потери из-за ошибки персонала и пользователей бывают?

- несанкционированное копирование, уничтожение или подделка информации
- потери при заражении системы компьютерными вирусами
+ случайное уничтожение или изменение данных
- сбои дисковых систем

Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии?

+ установка источников бесперебойного питания (UPS)
- Такого средства не существует
- Каждую минуту сохранять данные
- Перекидывать информацию на носитель, который не зависит от энергии

Способ защиты от сбоев процессора?

- установка источников бесперебойного питания (UPS)
+ симметричное мультипроцессирование
- Каждую минуту сохранять данные
- Перекидывать информацию на носитель, который не зависит от энергии

Симметричное мультипроцессирование

+ Способ защиты от сбоев процессора
- Способ защиты от сбоев устройств
- Каждую минуту копирование данных
- Не каждую минуту сохранение данных

Способ защиты от сбоев устройств для хранения информации?

- установка источников бесперебойного питания (UPS)
- симметричное мультипроцессирование
- Каждую минуту сохранять данные
+ Организация надежной и эффективной системы резервного копирования и дублирования данных

Средства защиты данных, функционирующие в составе программного обеспечения.

+ Программные средства защиты информации
- Технические средства защиты информации
- Источники бесперебойного питания (UPS)
- Смешанные средства защиты информации

Программные средства защиты информации.

+ средства архивации данных, антивирусные программы
- Технические средства защиты информации
- Источники бесперебойного питания (UPS)
- Смешанные средства защиты информации

Программное средство защиты информации.

+ криптография
- источник бесперебойного питания
- резервное копирование
- дублирование данных

Обеспечение достоверности и полноты информации и методов ее обработки.

- Конфиденциальность
+ Целостность
- Доступность
- Целесообразность

Обеспечение доступа к информации только авторизованным пользователям?

+ Конфиденциальность
- Целостность
- Доступность
- Целесообразность

Контрольная работа 1

1. СВЕДЕНИЯ (СООБЩЕНИЯ, ДАННЫЕ) НЕЗАВИСИМО ОТ ФОРМЫ ИХ ПРЕДСТАВЛЕНИЯ:
1. **Информация**
2. Информационные технологии
3. Информационная система
4. Информационно-телекоммуникационная сеть
5. Обладатель информации
2. ПРОЦЕССЫ, МЕТОДЫ ПОИСКА, СБОРА, ХРАНЕНИЯ, ОБРАБОТКИ, ПРЕДОСТАВЛЕНИЯ, РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ И СПОСОБЫ ОСУЩЕСТВЛЕНИЯ ТАКИХ ПРОЦЕССОВ И МЕТОДОВ:
1. Информация
2. **Информационные технологии**
3. Информационная система
4. Информационно-телекоммуникационная сеть
5. Обладатель информации
3. ЛИЦО, САМОСТОЯТЕЛЬНО СОЗДАВШЕЕ ИНФОРМАЦИЮ ЛИБО ПОЛУЧИВШЕЕ НА ОСНОВАНИИ ЗАКОНА ИЛИ ДОГОВОРА ПРАВО РАЗРЕШАТЬ ИЛИ ОГРАНИЧИВАТЬ ДОСТУП К ИНФОРМАЦИИ:
1. Источник информации
2. Потребитель информации
3. Уничтожитель информации
4. Носитель информации
5. **Обладатель информации**

4. ТЕХНОЛОГИЧЕСКАЯ СИСТЕМА, ПРЕДНАЗНАЧЕННАЯ ДЛЯ ПЕРЕДАЧИ ПО ЛИНИЯМ СВЯЗИ ИНФОРМАЦИИ, ДОСТУП К КОТОРОЙ ОСУЩЕСТВЛЯЕТСЯ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ЭТО:
1. База данных
2. Информационная технология
3. Информационная система
4. **Информационно-телекоммуникационная сеть**
5. Медицинская информационная система

5. ОБЯЗАТЕЛЬНОЕ ДЛЯ ВЫПОЛНЕНИЯ ЛИЦОМ, ПОЛУЧИВШИМ ДОСТУП К ОПРЕДЕЛЕННОЙ ИНФОРМАЦИИ, ТРЕБОВАНИЕ НЕ ПЕРЕДАВАТЬ ТАКУЮ ИНФОРМАЦИЮ ТРЕТЬИМ ЛИЦАМ БЕЗ СОГЛАСИЯ ЕЕ ОБЛАДАТЕЛЯ ЭТО:
1. Электронное сообщение
2. Распространение информации
3. Предоставление информации
4. **Конфиденциальность информации**
5. Доступ к информации
6. ДЕЙСТВИЯ, НАПРАВЛЕННЫЕ НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННЫМ КРУГОМ ЛИЦ ИЛИ ПЕРЕДАЧУ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННОМУ КРУГУ ЛИЦ ЭТО:
1. Уничтожение информации
2. **Распространение информации**
3. Предоставление информации
4. Конфиденциальность информации
5. Доступ к информации
8. ВОЗМОЖНОСТЬ ПОЛУЧЕНИЯ ИНФОРМАЦИИ И ЕЕ ИСПОЛЬЗОВАНИЯ ЭТО:
1. Сохранение информации
2. Распространение информации
3. Предоставление информации
4. Конфиденциальность информации
5. **Доступ к информации**

9. ИНФОРМАЦИЯ, ПЕРЕДАННАЯ ИЛИ ПОЛУЧЕННАЯ ПОЛЬЗОВАТЕЛЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ:
1. **Электронное сообщение**
2. Информационное сообщение
3. Текстовое сообщение
4. Визуальное сообщение
5. SMS-сообщение

10. ВСЕ КОМПОНЕНТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ, В КОТОРОМ НАКАПЛИВАЮТСЯ И ОБРАБАТЫВАЮТСЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ЭТО:
1. **Информационная система персональных данных**
2. База данных
3. Централизованное хранилище данных
4. Система Статэкспресс
5. Сервер

11. К СВЕДЕНИЯМ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА, СОГЛАСНО УКАЗУ ПРЕЗИДЕНТА РФ ОТ 6 МАРТА 1997 Г., ОТНОСЯТСЯ:
1. Информация о распространении программ
2. Информация о лицензировании программного обеспечения
3. Информация, размещаемая в газетах, Интернете
4. **Персональные данные**
5. Личная тайна

12. ОТНОШЕНИЯ, СВЯЗАННЫЕ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ, РЕГУЛИРУЮТСЯ ЗАКОНОМ…
1. «Об информации, информационных технологиях»
2. «О защите информации»
3. **Федеральным законом «О персональных данных»**
4. Федеральным законом «О конфиденциальной информации»
5. «Об утверждении перечня сведений конфиденциального характера»

13. ДЕЙСТВИЯ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ (СОГЛАСНО ЗАКОНУ), ВКЛЮЧАЯ СБОР, СИСТЕМАТИЗАЦИЮ, НАКОПЛЕНИЕ, ХРАНЕНИЕ, ИСПОЛЬЗОВАНИЕ, РАСПРОСТРАНЕНИЕ И Т. Д ЭТО:
1. «Исправление персональных данных»
2. «Работа с персональными данными»
3. «Преобразование персональных данных»
4. **«Обработка персональных данных»**
5. «Изменение персональных данных»

14. ДЕЙСТВИЯ, В РЕЗУЛЬТАТЕ КОТОРЫХ НЕВОЗМОЖНО ОПРЕДЕЛИТЬ ПРИНАДЛЕЖНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ КОНКРЕТНОМУ СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ:
1. Выделение персональных данных
2. Обеспечение безопасности персональных данных
3. Деаутентификация
4. Деавторизация
5. **Деперсонификация**

15. ПО РЕЖИМУ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПОДРАЗДЕЛЯЮТСЯ НА:
1. **Многопользовательские**
2. Однопользовательские
3. Без разграничения прав доступа
4. С разграничением прав доступа
5. Системы, не имеющие подключений

Контрольная работа 2

1.ПРОЦЕСС СООБЩЕНИЯ СУБЪЕКТОМ СВОЕГО ИМЕНИ ИЛИ НОМЕРА, С ЦЕЛЬЮ ПОЛУЧЕНИЯ ОПРЕДЕЛЁННЫХ ПОЛНОМОЧИЙ (ПРАВ ДОСТУПА) НА ВЫПОЛНЕНИЕ НЕКОТОРЫХ (РАЗРЕШЕННЫХ ЕМУ) ДЕЙСТВИЙ В СИСТЕМАХ С ОГРАНИЧЕННЫМ ДОСТУПОМ:
1. Авторизация

2. Аутентификация
3. Обезличивание
4. Деперсонализация
5. **Идентификация**

2.ПРОЦЕДУРА ПРОВЕРКИ СООТВЕТСТВИЯ СУБЪЕКТА И ТОГО, ЗА КОГО ОН ПЫТАЕТСЯ СЕБЯ ВЫДАТЬ, С ПОМОЩЬЮ НЕКОЙ УНИКАЛЬНОЙ ИНФОРМАЦИИ:

1. Авторизация
2. Обезличивание
3. Деперсонализация
4. **Аутентифика́ция**
5. Идентификация

3.ПРОЦЕСС, А ТАКЖЕ РЕЗУЛЬТАТ ПРОЦЕССА ПРОВЕРКИ НЕКОТОРЫХ ОБЯЗАТЕЛЬНЫХ ПАРАМЕТРОВ ПОЛЬЗОВАТЕЛЯ И, ПРИ УСПЕШНОСТИ, ПРЕДОСТАВЛЕНИЕ ЕМУ ОПРЕДЕЛЁННЫХ ПОЛНОМОЧИЙ НА ВЫПОЛНЕНИЕ НЕКОТОРЫХ (РАЗРЕШЕННЫХ ЕМУ) ДЕЙСТВИЙ В СИСТЕМАХ С ОГРАНИЧЕННЫМ ДОСТУПОМ

1. **Авториза́ция**
2. Идентификация
3. Аутентификация
4. Обезличивание
5. Деперсонализация

4.ПРОСТЕЙШИМ СПОСОБОМ ИДЕНТИФИКАЦИИ В КОМПЬЮТЕРНОЙ СИСТЕМЕ ЯВЛЯЕТСЯ ВВОД ИДЕНТИФИКАТОРА ПОЛЬЗОВАТЕЛЯ, КОТОРЫЙ ИМЕЕТ СЛЕДУЮЩЕЕ НАЗВАНИЕ:

1. Токен
2. Password
3. Пароль
4. **Login**
5. Смарт-карта

5.ОСНОВНОЕ СРЕДСТВО, ОБЕСПЕЧИВАЮЩЕЕ КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ, ПОСЫЛАЕМОЙ ПО ОТКРЫТЫМ КАНАЛАМ ПЕРЕДАЧИ ДАННЫХ, В ТОМ ЧИСЛЕ – ПО СЕТИ ИНТЕРНЕТ:

1. Идентификация
2. Аутентификация
3. Авторизация
4. Экспертиза
5. **Шифрование**

6.ДЛЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ ПО КАНАЛАМ ИНТЕРНЕТ ИСПОЛЬЗУЕТСЯ ТЕХНОЛОГИЯ:

1. WWW
2. DICOM
3. **VPN**
4. FTP
5. XML

7.КОМПЛЕКС АППАРАТНЫХ И/ИЛИ ПРОГРАММНЫХ СРЕДСТВ, ОСУЩЕСТВЛЯЮЩИЙ КОНТРОЛЬ И ФИЛЬТРАЦИЮ СЕТЕВОГО ТРАФИКА В СООТВЕТСТВИИ С ЗАДАННЫМИ ПРАВИЛАМИ И ЗАЩИЩАЮЩИЙ КОМПЬЮТЕРНЫЕ СЕТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА:

1. Антивирус
2. Замок
3. **Брандма́уэр**
4. Криптография
5. Экспертная система

8.ЗА ПРАВОНАРУШЕНИЯ В СФЕРЕ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЗАЩИТЫ ИНФОРМАЦИИ ДАННЫЙ ВИД НАКАЗАНИЯ НА СЕГОДНЯШНИЙ ДЕНЬ НЕ ПРЕДУСМОТРЕН:

1. Дисциплинарные взыскания
2. Административный штраф

3. Уголовная ответственность
4. Лишение свободы
5. **Смертная казнь**

9.НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ ЭТО:

1. **Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально**
2. Работа на чужом компьютере без разрешения его владельца
3. Вход на компьютер с использованием данных другого пользователя
4. Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей
5. Доступ к СУБД под запрещенным именем пользователя

10.«ПЕРСОНАЛЬНЫЕ ДАННЫЕ» ЭТО:

1. **Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу**
2. Фамилия, имя, отчество физического лица
3. Год, месяц, дата и место рождения, адрес физического лица
4. Адрес проживания физического лица
5. Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»

11.В ДАННОМ СЛУЧАЕ СОТРУДНИК УЧРЕЖДЕНИЯ МОЖЕТ БЫТЬ ПРИВЛЕЧЕН К ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:

1. Выход в Интернет без разрешения администратора
2. При установке компьютерных игр
3. В случаях установки нелицензионного ПО
4. В случае не выхода из информационной системы
5. **В любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности**

12.МОЖЕТ ЛИ СОТРУДНИК БЫТЬ ПРИВЛЕЧЕН К УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ:

1. Нет, только к административной ответственности
2. Нет, если это государственное предприятие
3. **Да**
4. Да, но только в случае, если действия сотрудника нанесли непоправимый вред
5. Да, но только в случае осознанных неправомочных действий сотрудника

13.ПРОЦЕДУРА, ПРОВЕРЯЮЩАЯ, ИМЕЕТ ЛИ ПОЛЬЗОВАТЕЛЬ С ПРЕДЪЯВЛЕННЫМ ИДЕНТИФИКАТОРОМ ПРАВО НА ДОСТУП К РЕСУРСУ ЭТО:

1. Идентификация
2. **Аутентификация**
3. Стратификация
4. Регистрация
5. Авторизация

14.НАИБОЛЕЕ ОПАСНЫМ ИСТОЧНИКОМ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ЯВЛЯЮТСЯ:

1. Другие предприятия (конкуренты)
2. Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам
3. **Рядовые сотрудники предприятия**
4. Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных
5. Хакеры

15.ВЫБЕРИТЕ, МОЖНО ЛИ В СЛУЖЕБНЫХ ЦЕЛЯХ ИСПОЛЬЗОВАТЬ ЭЛЕКТРОННЫЙ АДРЕС (ПОЧТОВЫЙ ЯЩИК), ЗАРЕГИСТРИРОВАННЫЙ НА ОБЩЕДОСТУПНОМ ПОЧТОВОМ СЕРВЕРЕ, НАПРИМЕР НА MAIL.RU:

1. **Нет, не при каких обстоятельствах**
2. Нет, но для отправки срочных и особо важных писем можно
3. Можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера

4. Можно, если информацию предварительно заархивировать с помощью программы winrar с паролем
5. Можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно

Контрольная работа 3

1.ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ, ДОСТУП К КОТОРОЙ ОГРАНИЧИВАЕТ В СООТВЕТСТВИИ С ЗАКОНАДЕЛЬСТВОМ РФ:

1. Информация составляющая государственную тайну
2. Информация составляющая коммерческую тайну
3. Персональная
4. **Конфиденциальная информация**
5. Документированная информация

2.ДЛЯ ТОГО ЧТОБЫ СНИЗИТЬ ВЕРОЯТНОСТЬ УТРАТЫ ИНФОРМАЦИИ НЕОБХОДИМО:

1. Регулярно производить антивирусную проверку компьютера
2. Регулярно выполнять проверку жестких дисков компьютера на наличие ошибок
3. **Регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты)**
4. Защитить вход на компьютер к данным паролем
5. Проводить периодическое обслуживание ПК

3.ПАРОЛЬ ПОЛЬЗОВАТЕЛЯ ДОЛЖЕН

1. **Содержать цифры и буквы, знаки препинания и быть сложным для угадывания**
2. Содержать только цифры
3. Содержать только буквы
4. Иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.)
5. Быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д.

4.ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЕСПЕЧИВАЕТ…

1. Блокирование информации
2. Искажение информации
3. **Сохранность информации**
4. Утрату информации
5. Подделку информации

5.ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ «О ГОСУДАРСТВЕННОЙ ТАЙНЕ» БЫЛ ПРИНЯТ В СЛЕДУЮЩЕМ ГОДУ:

1. 1982
2. 1985
3. 1988
4. **1993**
5. 2005

6.ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИЕЙ, ДОСТУП К КОТОРОЙ ОГРАНИЧЕН В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РФ, НАЗЫВАЕТСЯ

1. **Конфиденциальная**
2. Персональная
3. Документированная
4. Информация составляющая государственную тайну
5. Информация составляющая коммерческую тайну

7.ИНФОРМАЦИЯ ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЕ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ОПИСАНА В:

1. 1 главе Уголовного кодекса
2. 5 главе Уголовного кодекса
3. **28 главе Уголовного кодекса**
4. 100 главе Уголовного кодекса
5. 1000 главе Уголовного кодекса

8.В СТАТЬЕ 272 УГОЛОВНОГО КОДЕКСА ГОВОРИТСЯ…

1. **О неправомерном доступе к компьютерной информации**
2. О создании, исполнении и распространении вредоносных программ для ЭВМ
3. О нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

4. О преступлениях в сфере компьютерной информации
5. Об ответственности за преступления в сфере компьютерной информации

9.ФЕДЕРАЛЬНЫЙ ЗАКОН «ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ» НАПРАВЛЕН НА:

1. **Регулирование взаимоотношений в информационной сфере совместно с гражданским кодексом РФ**
2. Регулирование взаимоотношений в гражданском обществе РФ
3. Регулирование требований к работникам служб, работающих с информаций
4. Формирование необходимых норм и правил работы с информацией
5. Формирование необходимых норм и правил, связанных с защитой детей от информации

10.ХИЩЕНИЕ ИНФОРМАЦИИ – ЭТО…

1. **Несанкционированное копирование информации**
2. Утрата информации
3. Блокирование информации
4. Искажение информации
5. Продажа информации

11.ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ПЕРВОЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…

1. Государство
2. Коммерческая организация
3. **Муниципальное учреждение**
4. Любой гражданин
5. Группа лиц, имеющих общее дело

12.ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ВТОРОЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…

1. **Простые люди**
2. Государство
3. Коммерческая организация
4. Муниципальное учреждение
5. Некоммерческая организация

13.ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ТРЕТЬЕЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…

1. Люди
2. **Государство**
3. Муниципальное учреждение
4. Учреждение
5. Некоммерческая организация

14.ИНФОРМАЦИЕЙ, СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, ВЛАДЕЮТ:

1. **Государство**
2. Только образовательные учреждения
3. Только президиум Верховного Совета РФ
4. Граждане Российской Федерации
5. Только министерство здравоохранения

15.ИНФОРМАЦИЕЙ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ, ВЛАДЕЮТ:

1. Государство
2. **Различные учреждения**
3. Государственная Дума
4. Граждане Российской Федерации
5. Медико-социальные организации

Вопросы к зачету

1. Актуальность и основные задачи защиты информации. Основные понятия информационной безопасности.
2. Международные стандарты информационного обмена.
3. Асимметричные методы шифрования данных
4. Основные угрозы безопасности данных и их классификация.
5. Виды атак и методы взлома интрасетей злоумышленниками.
6. Три вида возможных нарушений информационной системы.
7. Симметричные методы шифрования данных.
8. Каналы утечки данных и их классификация

9. Идентификация, аутентификация пользователей. Классификация методов идентификации пользователей.
10. Уязвимые места информационных систем.
11. Обеспечение доступности данных
12. Основные методы защиты данных и их классификация
13. Защита информации в системах управления базами данных
14. Основные средства защиты данных и их классификация
15. Основные подходы к оценке и принципы оценки безопасности ИТ, используемые в TCSEC, ITSEC, РД Гостехкомиссии России. Сходство и различия
16. Формальные средства защиты информации
17. . Программно-технический аспект информационной безопасности
18. Неформальные средства защиты информации
19. Организационный аспект информационной безопасности
20. Мероприятия по защите информации от несанкционированного доступа
21. Управленческий аспект информационной безопасности
22. Мероприятия по защите информации от потерь
23. Законодательный аспект информационной безопасности
24. Мероприятия по защите информации от вредоносных программ
25. Вредоносные программы (вирусы) и их классификация.
26. Алгоритмы работы "компьютерных вирусов" и пути их внедрения в систему.
27. Индивидуальные признаки, используемые для определения "компьютерных вирусов" различных классов.
28. криптографическое преобразование информации, контроль и учет доступа
29. . Основные технологии построения защищенных ИС
30. Концепция информационной безопасности.
31. Классификация удаленных угроз в вычислительных сетях.
32. . Принципы защиты распределенных вычислительных сетей.

Тесты для проверки остаточных знаний

1.ПЕРСОНАЛЬНЫМИ ДАННЫМИ ВЛАДЕЮТ:
1. Государство
2. Различные учреждения
3. Государственная Дума
4. **Жители Российской Федерации**
5. Медико-социальные организации

2.ДОСТУП К ИНФОРМАЦИИ – ЭТО:
1. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
2. Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц
3. Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц
4. Информация, переданная или полученная пользователем информационно-телекоммуникационной сети
5. **Возможность получения информации и ее использования**

3.ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ, ДОСТУП К КОТОРОЙ ОГРАНИЧИВАЕТСЯ В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ ЭТО:
1. **Конфиденциальная информация**
2. Документы офера и договоров
3. Факс
4. Личный дневник
5. Законы РФ

4.ПЛАСТИКОВАЯ КАРТОЧКА, СОДЕРЖАЩАЯ ЧИП ДЛЯ КРИПТОГРАФИЧЕСКИХ ВЫЧИСЛЕНИЙ И ВСТРОЕННУЮ ЗАЩИЩЕННУЮ ПАМЯТЬ ДЛЯ ХРАНЕНИЯ ИНФОРМАЦИИ:

1. Токен
2. Password
3. Пароль
4. Login
5. **Смарт-карта**

5.УСТРОЙСТВО ДЛЯ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ, ПРЕДСТАВЛЯЮЩЕЕ СОБОЙ МОБИЛЬНОЕ ПЕРСОНАЛЬНОЕ УСТРОЙСТВО, НАПОМИНАЮЩИЕ МАЛЕНЬКИЙ ПЕЙДЖЕР, НЕ ПОДСОЕДИНЯЕМЫЕ К КОМПЬЮТЕРУ И ИМЕЮЩИЕ СОБСТВЕННЫЙ ИСТОЧНИК ПИТАНИЯ:

1. Токен
2. **Автономный токен**
3. USB-токен
4. Устройство iButton
5. Смарт-карта

6.ДОСТУП ПОЛЬЗОВАТЕЛЯ К ИНФОРМАЦИОННЫМ РЕСУРСАМ КОМПЬЮТЕРА И / ИЛИ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ ДОЛЖЕН РАЗРЕШАТЬСЯ ТОЛЬКО ПОСЛЕ:

1. Включения компьютера
2. **Идентификации по логину и паролю**
3. Запроса паспортных данных
4. Запроса доменного имени
5. Запроса ФИО

7.АППАРАТНЫЕ МОДУЛИ ДОВЕРЕННОЙ ЗАГРУЗКИ «АККОРД - АМДЗ» ПРЕДСТАВЛЯЮТ СОБОЙ…

1. **Аппаратный контролер**
2. Электронный замок
3. Система контроля
4. Сетевой адаптер
5. Копировальный аппарат

8.ЭЛЕКТРОННЫЕ ЗАМКИ «СОБОЛЬ» ПРЕДНАЗНАЧЕНЫ ДЛЯ …

1. **Обеспечения доверенной загрузки компьютера и контроля целостности файлов в системах**
2. Сканирования отпечатков пальцев
3. Проверки скорости и загрузки файлов
4. Общего контроля
5. Идентификации пользователя

55. Для защиты от злоумышленников необходимо использовать:

1. Системное программное обеспечение
2. Прикладное программное обеспечение
3. **Антивирусные программы**
4. Компьютерные игры
5. Музыку, видеофильмы

9.ФЕДЕРАЛЬНЫЙ ЗАКОН "ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ" ДАЕТ ОПРЕДЕЛЕНИЕ ИНФОРМАЦИИ:

1. Текст книги или письма
2. **Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления**
3. Сведения о явлениях и процессах
4. Факты и идеи в формализованном виде
5. Шифрованный текст, текст на неизвестном языке

10ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЕСТЬ ОБЕСПЕЧЕНИЕ…

1. Независимости информации
2. Изменения информации
3. Копирования информации
4. **Сохранности информации**
5. Преобразования информации

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).

Основная литература:

1. Петров С.В. Информационная безопасность. учебное пособие/ Петров С.В., Кисляков П.А.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с
2. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2014.— 702 с
3. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.— Электрон. текстовые данные.— Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 с

Дополнительная литература:

1. Аверченков В.И. Организационная защита информации. учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 с.
2. Башлы Информационная безопасность и защита информации / ЭБС ZNANIUM - Москва: Издательский Центр РИОР, 2011 - 222 с.
3. Мельников В.П. Информационная безопасность: Учебное пособие / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова - М.: Академия, 2011 - 336 с.

Перечень ресурсов информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), необходимых для освоения дисциплины (модуля).

1. http://www.cyberpolice.ru (Web-сервер подразделения по выявлению и пресечению преступлений, совершаемых с использованием поддельных кредитных карт, и преступлений, совершаемых путем несанкционированного доступа в компьютерные сети и базы данных)
2. http://www.infosecurity. report.ru/ (портал по информационной безопасности)
3. http://www.void.ru/ (портал по информационной безопасности)
4. http://www.infosec.ru/ (Сервер компании НИП «Информзащита»)
5. http://www.jetinfo.ru/ (Информационный бюллетень «Jet Info» с тематическим разделом по информационной безопасности)

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для обеспечения учебного процесса используются:

- лекционные аудитории и компьютерные классы ;
- персональные компьютеры;
- базовое программное обеспечение Windows

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций примерной ООП ВО по направлению 38.03.01 Экономика и профилю подготовки экономика предприятий и организаций

Рецензент от выпускающей кафедры (работодателя) по направлению

_____ _____

подпись И.О.Ф