ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ
ИМЕНИ ИМПЕРАТОРА ПЕТРА I»

Агроинженерный
наименование факультета
«Безопасности жизнедеятельности»
наименование кафедры

УТВЕРЖДАЮ
Зав.кафедрой
Высоцкая Е.А.
20.10.2015 г.

Фонд оценочных средств

по дисциплине **Б1.В.ОД.5 «Информационная безопасность предприятия»**
для подготовки магистров по направлению
35.04.06 Агроинженерия

Профиль подготовки "Инжиниринг безопасности труда на предприятии"
Уровень высшего образования – прикладная магистратура

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

Индекс	Формулировка	Разделы дисциплины						
		1	2	3	4	5	6	7
ОК- 3	готовностью к саморазвитию, самореализации, использованию творческого потенциала	+	+					
ОПК-3	способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения			+	+			
ПК-2	готовностью к организации технического обеспечения производственных процессов на предприятиях АПК					+	+	+

2. **Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания**

2.1 Шкала академических оценок освоения дисциплины

Виды оценок	Оценки	
Академическая оценка по 2-х балльной шкале (зачет)	не зачтено	зачтено

2.2 Текущий контроль

Код	Планируемые результаты	Раздел дисциплины	Содержание требования в разрезе разделов дисциплины	Технология формирования	Форма оценочного средства (контроля)	№Задания		
						Пороговый уровень (удовл.)	Повышенный уровень (хорошо)	Высокий уровень (отличные)
ОК - 3	*Знать сущность, цели и принципы безопасности предпринимательской деятельности, направления их практической реализации; -концепцию информационной безопасности, конституционные и законодательные основы ее реализации;*	*1, 2*	*Основные требования информационной безопасности. Составляющие национальных интересов Российской Федерации в информационной сфере. Стратегия национальной безопасности РФ. Доктрина информационной безопасности РФ. Понятие и сущность защиты информации. Цель защиты информации. Задачи защиты информации. Концептуальная модель информационной безопасности*	Лабораторные работы, самостоятельная работа, лекции	Устный опрос, собеседование, *Тестирование,* реферат	*Тесты из-задания 3.3 (V1, V2) Задание из раздела 3.4*	*Тесты из-задания 3.3 (V1, V2) Задание из раздела 3.4*	*Тесты из-задания 3.3 (V1, V2) Задание из раздела 3.4*
ОПК-3	*Знать* основные требования информационной безопасности	*3,4*	Законодательство Российской Федерации в области информационной безопасности. Нормативно-правовые основы информационной безопасности РФ. Ответственность за нарушения в сфере информационной безопасности РФ. Предмет защиты информации. Энтропийный подход для измерения количества информации.	Лабораторные работы, самостоятельная работа, лекции	Устный опрос, собеседование Тестирование, реферат	*Тесты из-задания 3.3 (V3, V4) Задание из раздела 3.4*	*Тесты из-задания 3.3 (V3, V4) Задание из раздела 3.4*	*Тесты из-задания 3.3 (V3, V4) Задание из раздела 3.4*

			Тезаурусный и практический подходы для измерения количества информации. Информация как объект права собственности. Объект защиты информации и информационная система.					
ПК-2	*Знать* функциональные возможности и предпосылки эффективного использования различных типов технологических систем и способов обработки и хранения традиционных и электронных конфиденциальных документов; -механизмы реализации атак в сетях, реализующих протоколы Интернет транспортного и сетевого уровня; -основные протоколы идентификации и аутентификации абонентов сети; -защитные механизмы и средства обеспечения сетевой безопасности; -средства и методы	*5,6,7*	Случайные угрозы. Сбой и отказы сложных систем. Ошибки при разработке информационной системы. Преднамеренные угрозы. Классификация нарушителей информационной безопасности. Анализ компьютерных преступлений. Н. Компьютерные мошенничества. Вредоносное программное обеспечение. Компьютерные вирусы. Программные закладки и троянские программы. Антивирусное программное обеспечение.	Лабораторные работы, самостоятельная работа, лекции	Устный опрос, собеседование Тестирование, реферат	*Тесты из-задания 3.3 (V5, V6, V7) Задание из раздела 3.4*	*Тесты из-задания 3.3 (V5, V6, V7) Задание из раздела 3.4*	*Тесты из-задания 3.3 (V5, V6, V7) Задание из раздела 3.4*

	предотвращения и обнаружения вторжений; -основные виды политик управления доступом и информационными потоками в компьютерных системах;							

2.3 Промежуточная аттестация

Код	Планируемые результаты	Технология формирования	Форма оценочного средства (контроля)	№Задания		
				Пороговый уровень (удовл.)	Повышенный уровень (хорошо)	Высокий уровень (отлично)
ОК-3	*Знать* -сущность, цели и принципы безопасности предпринимательской деятельности, направления их практической реализации; -концепцию информационной безопасности, конституционные и законодательные основы ее реализации; *Уметь* -использовать основы полученных знаний в различных сферах жизнедеятельности *Иметь навыки* опыт и методы работы с персоналом, обладающим конфиденциальной	*Лабораторные работы, самостоятельная работа, лекции*	*зачет*	*Задания из раздела 3.1 (1-2 5-6)*	*Задания из раздела 3.1 (1-3 5-7)*	*Задания из раздела 3.1 (1-4 5-8)*

	информацией					
ОПК-3	*Знать* -основные требования информационной безопасности; *Уметь* в соответствии законодательством Российской Федерации в области информационной безопасности, нормативно-правовыми основами информационной безопасности РФ предпринимать сложные решения в различных нестандартных ситуациях; с помощью различных методов оценивать количество информации. Ее состав *Иметь навыки* использования полученных знаний и основ в практической деятельности	*Лабораторные работы, самостоятельная работа, лекции*	*зачет*	*Задания из раздела 3.1 (9-12 16-18)*	*Задания из раздела 3.1 (9-14 16-19)*	*Задания из раздела 3.1 (9-15 16-20)*
ПК-2	*Знать* функциональные возможности и предпосылки эффективного использования различных типов технологических систем и способов обработки и хранения традиционных и электронных конфиденциальных документов; *Уметь* осуществлять анализ компьютерных преступлений, вредоносного программного обеспечения. компьютерных вирусов;	*Лабораторные работы, самостоятельная работа, лекции*	*зачет*	*Задания из раздела 3.1 (21-23 26-29 33-38)*	*Задания из раздела 3.1 (21-24 26-30 33-40)*	*Задания из раздела 3.1 (21-25 26-32 33-43)*

	выявлять нарушителей информационной безопасности; организовывать защиту информационных систем. *Иметь навыки* конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; анализа результатов работы средств обнаружения вторжений					

2.4 Критерии оценки на экзамене

Не предусмотрено

2.5 Критерии оценки на зачёте

Оценка экзаменатора, уровень	Критерии
«зачтено», пороговый уровень	Обучающийся показал знание основных положений учебной дисциплины, умение получить с помощью преподавателя правильное решение конкретной практической задачи из числа предусмотренных рабочей программой, знакомство с рекомендованной справочной
«незачтено»,	При ответе обучающегося выявились существенные пробелы в знаниях основных положений учебной дисциплины, неумение с помощью преподавателя получить правильное решение конкретной практической задачи из числа предусмотренных рабочей программой учебной дисциплины, слабо знает рекомендованную литературу

2.6 Критерии оценки устного опроса

Оценка	Критерии
«отлично»	выставляется обучающемуся, если он четко выражает свою точу зрения по рассматриваемым вопросам, приводя соответствующие примеры
«хорошо»	выставляется обучающемуся, если он допускает отдельные погрешности в ответе
«удовлетворительно»	выставляется обучающемуся, если он обнаруживает пробелы в знаниях основного учебно-программного материала
«неудовлетворительно»	выставляется обучающемуся, если он обнаруживает существенные пробелы в знаниях основных положений учебной дисциплины, неумение с помощью преподавателя получить правильное решение конкретной практической задачи из числа предусмотренных рабочей программой учебной дисциплины

2.7 Критерии оценки тестов

Ступени уровней освоения компетенций	Отличительные признаки	Показатель оценки сформированной компетенции
Пороговый	Обучающийся воспроизводит термины, основные понятия, способен узнавать языковые явления.	Не менее 55 % баллов за задания теста.
Продвинутый	Обучающийся выявляет взаимосвязи, классифицирует, упорядочивает, интерпретирует, применяет на практике пройденный материал.	Не менее 75 % баллов за задания теста.
Высокий	Обучающийся анализирует,	Не менее 90 % баллов

	оценивает, прогнозирует, конструирует.	за задания теста.
Компетенция не сформирована		Менее 55 % баллов за задания теста.

2.8 Критерии оценки решения задач

Условия оценки теста	
Предел длительности контроля знаний	45 мин.
Предлагаемое количествозадач	1-2
Последовательность выборки тем	Согласно изучаемой теме
Критерии оценки:	
3 балла	Решена верно
2 балла	Решена с незначительными ошибками, присутствует логика решения.
1 балл	Решение начато, но не закончено
0 баллов	Не решена

2.9 Критерии оценки реферата

Изложенное понимание реферата как целостного авторского текста определяет критерии его оценки: новизна текста; обоснованность выбора источника; степень раскрытия сущности вопроса; соблюдения требований к оформлению.

Новизна текста: а) актуальность темы исследования; б) новизна и самостоятельность в постановке проблемы, формулирование нового аспекта известной проблемы в установлении новых связей (межпредметных, внутрипредметных, интеграционных); в) умение работать с исследованиями, критической литературой, систематизировать и структурировать материал; г) явленность авторской позиции, самостоятельность оценок и суждений; д) стилевое единство текста, единство жанровых черт.

Степень раскрытия сущности вопроса: а) соответствие плана теме реферата; б) соответствие содержания теме и плану реферата; в) полнота и глубина знаний по теме; г) обоснованность способов и методов работы с материалом; е) умение обобщать, делать выводы, сопоставлять различные точки зрения по одному вопросу (проблеме).

Обоснованность выбора источников: а) оценка использованной литературы: привлечены ли наиболее известные работы по теме исследования (в т.ч. журнальные публикации последних лет, последние статистические данные, сводки, справки и т.д.).

Соблюдение требований к оформлению: а) насколько верно оформлены ссылки на используемую литературу, список литературы; б) оценка грамотности и культуры изложения (в т.ч. орфографической, пунктуационной, стилистической культуры), владение терминологией; в) соблюдение требований к объёму реферата.

Оценка	Критерии
«зачтено»	если выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий

	анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.
«не зачтено»	тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

2.10 Допуск к сдаче зачета

1.*Посещение занятий. Допускается один пропуск без предъявления справки.*
2. Выполнение домашних заданий.
3. Активное участие в работе на занятиях.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

3.1 Вопросы к зачету

1. Основные понятия и определения информационной безопасности.
2. Составляющие национальных интересов Российской Федерации в информационной сфере
3. Стратегия национальной безопасности РФ.
4. Понятие и назначение доктрины информационной безопасности. Основные положения доктрины информационной безопасности Российской Федерации и их реализация.
5. Сущность и понятие защиты информации.
6. Уязвимость информации. Цели защиты информации.
7. Задачи защиты информации.
8. Концептуальная модель информационной безопасности
9. Законодательство Российской Федерации в области информационной безопасности.
10. Подзаконные нормативно-правовые акты в сфере защиты информации.
11. Понятие и виды конфиденциальной информации в современном российском законодательстве.
12. Государственная тайна, ее нормативное регулирование.
13. Правовой режим персональных данных. Общая характеристика Федерального закона «О персональных данных»
14. Понятие коммерческой тайны. Общая характеристика Федерального закона «О коммерческой тайне».
15. Ответственность за нарушения в сфере информационной безопасности РФ.
16. Предмет защиты информации.
17. Объект защиты информации и информационная система.
18. Энтропийный подход для измерения количества информации.
19. Тезаурусный и практический подходы для измерения количества информации.
20. Информация как объект права собственности.
21. Угрозы информационной безопасности.

22. Случайные угрозы. Сбой и отказы сложных систем. Ошибки при разработке информационной системы.
23. Преднамеренные угрозы.
24. Модель гипотетического нарушителя информационной безопасности.
25. Нарушитель и злоумышленник. Классификация нарушителей информационной безопасности.
26. Анализ компьютерных преступлений.
27. Несанкционированный доступ и перехват информации.
28. Изменение информации.
29. Компьютерные мошенничества.
30. Вредоносное программное обеспечение. Компьютерные вирусы. Программные закладки и троянские программы.
31. Антивирусное программное обеспечение. Виды антивирусных программ.
32. Методы и средства защиты от вредоносных программ
33. Методы и средства защиты информации.
34. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
35. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
36. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации
37. Разграничение доступа к данным в ОС
38. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
39. Понятие атаки на систему информационной безопасности. Особенности локальных атак.
40. Распределенные информационные системы. Удаленные атаки на информационную систему.
41. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
42. Физические средства обеспечения информационной безопасности.
43. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.
44. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
45. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.

.

Практические задачи

Задача №1 Установить политику аудита в Windows 7.

Задача №2 Настроить разрешения к доступу данных Windows 7,8.

Задача №3 Создать и настроить учетную запись пользователя ПК.

Задача №4 Показать умение управления диспетчером сертификатов в Windows 7,8.

Задача №5 Настроить параметры безопасности web-браузера.

Задача №6 Установить политику IP-безопасности на ПК.

Задача №7 Выбрать и установить шаблоны безопасности в Windows 7,8.

Задача №8 Осуществить анализ и настройку системы защиты Windows.

Задача №9 Восстановить файл, зараженный макровирусом.

Задача №10 Проверить потенциальные места записей «троянских программ» в системном реестре ОС Windows.

Задача №11 Разработать систему правил по управлению входящими сообщениями в Outlook Express и настроить Outlook Express для передачи сообщений с электронной цифровой подписью.

Задача №12 Настроить параметры локальной политики безопасности операционной системы Windows 7,8.

Задача №13 Включить и отключить шифрование файлов шифрующей файловой системой EFS. Экспортировать сертификат с ключами для расшифровки файлов на другом компьютере.

3.2. Вопросы к экзамену

Не предусмотрено

3.3 Тестовые задания»

V1 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1. **Сложность обеспечения информационной безопасности является следствием:**

злого умысла разработчиков информационных систем
√объективных проблем современной технологии программирования
происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы

2. **Что из перечисленного не относится к числу основных аспектов информационной безопасности:**

доступность
целостность
√защита от копирования
конфиденциальность

3. **В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:**

√законодательные меры
меры обеспечения доступности
профилактические меры

4. **Что из перечисленного относится к числу основных аспектов информационной безопасности:**

подотчетность - полнота регистрационной информации о действиях субъектов
приватность - сокрытие информации о личности пользователя
√конфиденциальность - защита от несанкционированного ознакомления

5. **Меры информационной безопасности направлены на защиту от:**

√нанесения неприемлемого ущерба
нанесения любого ущерба
подглядывания в замочную скважину

6. **Что из перечисленного не относится к числу основных аспектов информационной безопасности:**

доступность
√масштабируемость
целостность
конфиденциальность

7. **Сложность обеспечения информационной безопасности является следствием:**

невнимания широкой общественности к данной проблематике
все большей зависимости общества от информационных систем
√быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним

8. **Что понимается под информационной безопасностью:**

защита душевного здоровья телезрителей
√защита от нанесения неприемлемого ущерба субъектам информационных отношений
обеспечение информационной независимости России

V2 ОБЩЕЕ СОДЕРЖАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

9. **Необходимость объектно-ориентированного подхода к информационной безопасности является следствием того, что:**

√с программно-технической точки зрения, информационная безопасность - ветвь информационных технологий и должна развиваться по тем же законам
объектно-ориентированный подход популярен в академических кругах
объектно-ориентированный подход поддержан обширным инструментарием

10. **Что означает термин ДОСТУПНОСТЬ ИНФОРМАЦИИ?**

√Это свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

Это свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Это подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению ее конфиденциальности, целостности, доступности, или неправомерному ее тиражированию.

11. **Что означает термин ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ?**

√Это свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Это свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

Это подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению ее конфиденциальности, целостности, доступности, или неправомерному ее тиражированию.

12. **В чем заключается конфиденциальность компонента системы?**

√В том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

В том, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права.

В том, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

13. **В чем заключается целостность компонента системы?**

√В том, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права.

В том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

В том, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

14. **В чем заключается доступность компонента системы?**

√В том, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

В том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

В том, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права.

15. **Выявление неадекватного поведения выполняется системами управления путем применения методов, типичных для:**

систем анализа защищенности
√систем активного аудита
систем идентификации

16. **В число уровней, на которых группируются меры обеспечения информационной безопасности, входят:**

√законодательный
исполнительный
судебный

17. В число направлений повседневной деятельности на процедурном уровне входят:

√резервное копирование
√управление носителями
изготовление резервных носителей

18. В число классов мер процедурного уровня входят:

√управление персоналом
управление персоналками
√реагирование на нарушения режима безопасности

19. Агрессивное потребление ресурсов является угрозой:

√доступности
конфиденциальности
целостности

20. В число принципов управления персоналом входят:

"разделяй и властвуй"
√разделение обязанностей
инкапсуляция наследования

V3 ЗАКОНОДАТЕЛЬНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РФ.

21. Уголовный кодекс РФ не предусматривает наказания за:

√увлечение компьютерными играми в рабочее время
неправомерный доступ к компьютерной информации
нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

22. Уголовный кодекс РФ не предусматривает наказания за:

неправомерный доступ к компьютерной информации
создание, использование и распространение вредоносных программ
√массовую рассылку незапрошенной рекламной информации

23. Большинство людей не совершают противоправных действий потому, что это:

√осуждается и/или наказывается обществом
технически невозможно
сулит одни убытки

24. Согласно стандарту X.700, в число функций управления безопасностью входят:

создание инцидентов
√реагирование на инциденты
устранение инцидентов

25. На современном этапе развития законодательного уровня информационной безопасности в России важнейшее значение имеют:

меры ограничительной направленности
√направляющие и координирующие меры
меры по обеспечению информационной независимости

26. Согласно рекомендациям X.800, выделяются следующие сервисы безопасности:

√аутентификация
идентификация
туннелирование

27. Уровень безопасности С, согласно "Оранжевой книге", характеризуется:

√произвольным управлением доступом
принудительным управлением доступом
верифицируемой безопасностью

V4 ПРЕДМЕТ И ОБЪЕКТ ЗАЩИТЫ ИНФОРМАЦИИ.

28. В число принципов физической защиты входят:

беспощадный отпор
√непрерывность защиты в пространстве и времени
минимизация защитных средств

29. В число направлений физической защиты входят:

√противопожарные меры
межсетевое экранирование
контроль защищенности

30. Что означает термин ПРАВОВЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

√Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.

Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации.

Это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации.

Это разного рода механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам АС и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации.

Это различные электронные устройства и специальные программы, входящие в состав АС, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

31. Что означает термин ОРГАНИЗАЦИОННЫЕ (АДМИНИСТРАТИВНЫЕ) МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ?

√Это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации.

Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.

Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации.

Это разного рода механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам АС и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации.

Это различные электронные устройства и специальные программы, входящие в состав АС, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

32. Что означает термин ТЕХНИЧЕСКИЕ (АППАРАТНО-ПРОГРАММНЫЕ) СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ?

√Это различные электронные устройства и специальные программы, входящие в состав АС, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты

информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.

Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации.

Это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации.

Это разного рода механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам АС и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации.

V5 УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

33. Самыми опасными угрозами являются:

√непреднамеренные ошибки штатных сотрудников
вирусные инфекции
атаки хакеров

34. Компьютерная преступность в мире:

остается на одном уровне
снижается
√растет

35. Системы анализа защищенности помогают:

оперативно пресечь известные атаки
√предотвратить известные атаки
восстановить ход известных атак

36. Агрессивное потребление ресурсов является угрозой:

√доступности
конфиденциальности
целостности

37. Кто является хакером?

Это лица, проявляющие чрезмерный интерес к устройству сложных систем, как правило компьютерных, и в следствии этого интереса обладающие большими познаниями по части архитектуры и принципов

устройства вычислительной среды или технологии телекоммуникаций, что используется для похищения информации.

√Это лица, изучающие систему с целью ее взлома. Они реализуют свои криминальные наклонности в похищении информации и написании разрушающего программного обеспечения и вирусов, при этом применяют различные способы атак на компьютерную систему, используя принципы построения протоколов сетевого обмена.

Это лица, которые «взламывая» интрасети, получают информацию о топологии этих сетей, используемых в них программно-аппаратных средствах и информационных ресурсах, а также реализованных методах защиты. Эти сведения они продают заинтересованным лицам.

38. Как классифицируются виды угроз информации по природе возникновения?

√Стихийные бедствия, несчастные случаи, ошибки обслуживающего персонала и пользователей, злоупотребления обслуживающего персонала и пользователей, злоумышленные действия нарушителей, сбои и отказы оборудования.

Угрозы персоналу, информации, информационным системам, материальным, финансовым, информационным данным.

Угрозы информационным системам, материальным, финансовым, информационным данным, злоумышленные действия нарушителей, сбои и отказы оборудования.

39. Как классифицируются виды угроз информации по ориентации на ресурсы?

√Угрозы персоналу, информации, информационным системам, материальным, финансовым, информационным данным.

Стихийные бедствия, несчастные случаи, ошибки обслуживающего персонала и пользователей, злоупотребления обслуживающего персонала и пользователей, злоумышленные действия нарушителей, сбои и отказы оборудования.

Угрозы информационным системам, материальным, финансовым, информационным данным, злоумышленные действия нарушителей, сбои и отказы оборудования.

40. Какие угрозы информации относятся к искусственным?

√ошибки человека как звена системы;
схемные и системотехнические ошибки разработчиков;
структурные, алгоритмические и программные ошибки;
действия человека, направленные на несанкционированные воздействия на информацию.

отказы и сбои аппаратуры;
помехи на линиях связи от воздействий внешней среды;
аварийные ситуации;
стихийные бедствия.

аварийные ситуации;
стихийные бедствия;
ошибки человека как звена системы;
схемные и системотехнические ошибки разработчиков.

41. Какие угрозы информации относятся к случайным?

√проявление ошибок программно-аппаратных средств АС;
некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;

неправомерное включение оборудования или изменение режимов работы устройств и программ;
неумышленная порча носителей информации;
пересылка данных по ошибочному адресу абонента (устройства).

несанкционированное чтение информации;
несанкционированное изменение информации;
несанкционированное уничтожение информации;
полное или частичное разрушение операционной системы.

пересылка данных по ошибочному адресу абонента (устройства);
ввод ошибочных данных;
несанкционированное уничтожение информации; полное или частичное разрушение операционной системы.

42. Какие угрозы информации относятся к преднамеренным?

√несанкционированное чтение информации;
несанкционированное изменение информации;
несанкционированное уничтожение информации; полное или
частичное разрушение операционной системы.

проявление ошибок программно-аппаратных средств АС;
некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
неправомерное включение оборудования или изменение режимов работы устройств и программ;
неумышленная порча носителей информации; пересылка данных по ошибочному адресу абонента (устройства).

пересылка данных по ошибочному адресу абонента (устройства); ввод ошибочных данных;
несанкционированное уничтожение информации; полное или частичное разрушение операционной системы.

43. Источником каких угроз информации являются несанкционированные программно-аппаратные средства?

√нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным

расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
заражение компьютера вирусами с деструктивными функциями.

.внедрение агентов в число персонала системы;
вербовка персонала или отдельных пользователей, имеющих определенные полномочия; угроза несанкционированного копирования секретных данных пользователем; разглашение, передача или утрата атрибутов разграничения доступа.

запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.); возникновение отказа в работе операционной системы.

V6 КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ И ИХ ОСОБЕННОСТИ

44. Какими основными свойствами обладает компьютерный вирус?

способностью к созданию собственных копий;
наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы.

способностью к созданию собственных копий;
способностью уничтожать информацию на дисках;
способность создавать всевозможные видео и звуковые эффекты.

√наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы;
способностью оставлять в оперативной памяти свою резидентную часть;
способностью вируса полностью или частично скрыть себя в системе.

45. В чем заключается принцип работы файлового вируса?

Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы;

записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор.

√Вирусы заражают файлы-документы и электронные таблицы популярных редакторов.

Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

46. В чем заключается принцип работы загрузочного вируса?

√Вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор.

Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы;

Вирусы заражают файлы-документы и электронные таблицы популярных редакторов.

Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

47. В чем заключается принцип работы макровируса?

Вирусы заражают файлы-документы и электронные таблицы популярных редакторов.

√Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы;

Вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор.

Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

48. В чем заключается принцип работы сетевого вируса?

√Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы;

Вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор.

Вирусы заражают файлы-документы и электронные таблицы популярных редакторов.

49. На чем основан алгоритм работы резидентного вируса?

√Вирус при инфицировании компьютера оставляет в оперативной памяти свою часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Эти вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки ОС.

Использование этих алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным алгоритмом является перехват запросов ОС на чтение-запись зараженных объектов и затем вирусы либо временно лечат их, либо подставляют вместо себя незараженные участки информации.

Используются для того, чтобы максимально усложнить процедуру обнаружения вируса. Эти вирусы достаточно трудно поддаются обнаружению, они не имеют сигнатур, т.е. не содержат ни одного постоянного участка кода. В большинстве случаев два образца одного и того же вируса не будут иметь ни одного совпадения.

50. По деструктивным возможностям, как влияют на работу компьютера безвредные вирусы?

√Никак не влияющие на работу компьютера кроме уменьшения свободной памяти на диске в результате своего распространения.

Влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами.

Могут привести к серьезным сбоям в работе компьютера.

В алгоритм работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти.

51. По деструктивным возможностям, как влияют на работу компьютера неопасные вирусы?

√Влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами.

Никак не влияющие на работу компьютера кроме уменьшения свободной памяти на диске в результате своего распространения.

Могут привести к серьезным сбоям в работе компьютера.

В алгоритм работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти.

V7 СИСТЕМНОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ.

52. Аутентификация на основе пароля, переданного по сети в зашифрованном виде, плоха, потому что не обеспечивает защиты от:

перехвата
√воспроизведения
√атак на доступность

53. При использовании сервера аутентификации Kerberos пароли по сети:

√не передаются
передаются в зашифрованном виде
передаются в открытом виде

54. Цифровой сертификат содержит:

ЭЦП пользователя
√ЭЦП доверенного центра
ЭЦП генератора криптографических ключей

55. Протоколирование само по себе не может обеспечить неотказуемость, потому что:

регистрационная информация может быть рассредоточена по разным сервисам и разным компонентам распределенной ИС
√целостность регистрационной информации может быть нарушена
должна соблюдаться конфиденциальность регистрационной информации, а проверка неотказуемости нарушит конфиденциальность

56. Криптография необходима для реализации следующих сервисов безопасности:

√шифрование
туннелирование
разграничение доступа

57. На межсетевые экраны целесообразно возложить следующие функции:

√антивирусный контроль "на лету"
антивирусный контроль компьютеров внутренней сети
антивирусный контроль компьютеров внешней сети

58. Экранирование на сетевом уровне может обеспечить:

√разграничение доступа по сетевым адресам
выборочное выполнение команд прикладного протокола
контроль объема данных, переданных по TCP-соединению

59. Аутентификация на основе пароля, переданного по сети в зашифрованном виде и снабженного открытой временной меткой, плоха, потому что не обеспечивает защиты от:

перехвата
√воспроизведения
√атак на доступность

60. В число целей политики безопасности верхнего уровня входят:

√формулировка административных решений по важнейшим аспектам реализации программы безопасности

выбор методов аутентификации пользователей
√обеспечение базы для соблюдения законов и правил

61. <u>В число универсальных сервисов безопасности входят:</u>

√шифрование
средства построения виртуальных частных сетей
√туннелирование

62. <u>В число принципов управления персоналом входят:</u>

"разделяй и властвуй"
√разделение обязанностей
инкапсуляция наследования

3.4 Перечень тем рефератов.

1. Особенности информации передаваемой по открытым телекоммуникационным сетям.
2. Государственная тайна – элемент информационной безопасности государства.
3. Конфиденциальная информация: понятие и еѐ виды. Правовое регулирование конфиденциальной информации в сфере обеспечения информационной безопасности.
4. Деятельность в сфере информации, требующая лицензирования. Аттестация объектов информатизации. Особенности сертификации средств защиты информации по требованиям безопасности.
5. Защита объектов интеллектуальных прав в системе правового регулирования информационной безопасности.
6. Понятие и виды юридической ответственности за нарушения в области информационной безопасности. Особенности юридической ответственности в области трудовых отношений.
7. Факторы, оказывающие влияние на информационную безопасность в политической, экономической, военной, культурной и нравственной сферах деятельности Российской Федерации.

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

4.1 Положение о формах, периодичности и порядке проведения текущего контроля успеваемости и промежуточной аттестации обучающихся П ВГАУ 1.1.05 – 2014

4.2 Методические указания по проведению текущего контроля

1.	Сроки проведения текущего контроля	*На лабораторных занятиях*
2.	Место и время проведения текущего контроля	В учебной аудитории в течение лабораторного занятия
3.	Требования к техническому	в соответствии с ОПОП и рабочей программой

	оснащению аудитории	
4.	Ф.И.О. преподавателя (ей), проводящих процедуру контроля	*Андрианов А.А.*
5.	Вид и форма заданий	*лабораторная работа, самостоятельная работа*
6.	Время для выполнения заданий	*в течение занятия*
7.	Возможность использований дополнительных материалов.	*Обучающийся может пользоваться дополнительными материалами*
8.	Ф.И.О. преподавателя (ей), обрабатывающих результаты	*Андрианов А.А.*
9.	Методы оценки результатов	*Экспертный*
10.	Предъявление результатов	*Оценка выставляется в журнал/доводится до сведения обучающихся в течение занятия*
11.	Апелляция результатов	*В порядке, установленном нормативными документами, регулирующими образовательный процесс в Воронежском ГАУ*