Министерство сельского хозяйства Российской Федерации
Департамент научно-технологической политики и образования
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Красноярский государственный аграрный университет»

СОГЛАСОВАНО:
Директор ИЭиУ АПК
Шапорова З.Е.
«_27_» _марта_ 2025 г.

УТВЕРЖДАЮ:
Ректор
Пыжикова Н.И.
«_28_» _марта_ 2025 г.

ДОКУМЕНТ ПОДПИСАН
УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ВЫДАННОЙ: ФГБОУ ВО КРАСНОЯРСКИЙ ГАУ
ВЛАДЕЛЕЦ: РЕКТОР ПЫЖИКОВА Н.И.
ДЕЙСТВИТЕЛЕН: 15.05.2025 - 08.08.2026

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
(текущего оценивания, промежуточной аттестации)

Институт Экономики и управления АПК
Кафедра Информационные технологии и математическое обеспечение информационных систем
Наименование и код ОПОП: 09.04.03 «Прикладная информатика»
Направленность (профиль): Цифровые технологии в АПК
Дисциплина: **Технологии защиты информации в компьютерных сетях**

Красноярск 2025

Составитель: Титовская Н.В., к.т.н., доцент
(ФИО, ученая степень, ученое звание)

«05» марта 2025 г.

Эксперт: Середкин В.Г.к.т.н., доцент
(ФИО, ученая степень, ученое звание)

«05» марта 2025 г.

ФОС разработан в соответствии с рабочей программой дисциплины.

ФОС обсужден на заседании кафедры Информационные технологии и математическое обеспечение информационных систем протокол
№ 7 «21» марта 2025 г.

Зав. кафедрой Калитина Вера Владимировна, к.п.н., доцент
(ФИО, ученая степень, ученое звание)

«21» марта 2025 г.

ФОС принят методической комиссией института Экономики и управления
АПК протокол № 7 «24» марта 2025 г.

Председатель методической комиссии Рожкова А.В.

«24» марта 2025 г.

Содержание

1 Цель и задачи фонда оценочных средств

Целью создания ФОС дисциплины «Технологии защиты информации в компьютерных сетях» является установление соответствия учебных достижений запланированным результатам обучения и требованиям образовательных программ и рабочих программ модулей

ФОС по дисциплине решает задачи:

- контроль и управление процессом приобретения магистрантами необходимых знаний, умений, навыков и уровня сформированности компетенции, определѐнных в ФГОС ВО по направлению 09.04.03 «Технологии защиты информации в компьютерных сетях»;
- контроль и управление достижением целей реализации ОПОП, определенных в виде набора общепрофессиональных компетенций выпускников;
- обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс университета.

Назначение фонда оценочных средств: используется для оперативного и регулярного управления учебной деятельностью (в том числе самостоятельной) магистрантов. А также предназначен для оценки степени достижения запланированных результатов обучения по завершению изучения дисциплины «Технологии защиты информации в компьютерных сетях» в установленной учебным планом форме в 4 семестре –зачетом с оценкой.

2 Нормативные документы

ФОС разработан на основе Федерального государственного образовательного стандарта высшего образования по направлению подготовки **09.04.03** «Прикладная информатика», рабочей программы дисциплины «Технологии защиты информации в компьютерных сетях».

3 Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины. Формы контроля формирования компетенций.

Компетенция	Этап формирования компетенции	Образовательные технологии	Тип контроля	Форма контроля
Способен управлять проектом на всех этапах его жизненного цикла с учетом основных требований технологии защиты информации в компьютерных сетях (УК-2)	теоретический (информационный)	лекции, самостоятельная работа	текущий	Опрос, тестирование
	практико-ориентированный	лабораторные работы, самостоятельная работа	текущий	Контроль правильности выполнения лабораторных работ
	оценочный	аттестация	промежуточный	зачет с оценкой
Способность использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС(ПК-5)	теоретический (информационный)	лекции, самостоятельная работа	текущий	Опрос, тестирование
	практико-ориентированный	лабораторные работы, самостоятельная работа	текущий	Контроль правильности выполнения лабораторных работ

	оценочный	аттестация	промежуточный	зачет с оценкой

4 Показатели и критерии оценивания компетенций

Таблица 4.1 – Показатели и критерии оценки результатов обучения

Показатель оценки результатов обучения	**Критерий оценки результатов обучения**
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	
Пороговый уровень	Разрабатывает концепцию проекта в рамках обозначенной проблемы: формулирует цель, задачи, обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения
Продвинутый уровень	Способен разрабатывать и анализировать альтернативные варианты проектов для достижения намеченных результатов; разрабатывать проекты, определять целевые этапы и основные направления работ
Высокий уровень	Предлагает процедуры и механизмы оценки качества проекта, инфраструктурные условия для внедрения результатов проекта
ПК-5 Способность использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС	
Пороговый уровень	Понимает передовые методы оценки качества, надежности и информационной безопасности ИС
Продвинутый уровень	Способен использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС
Высокий уровень	Применяет передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС

Таблица 4.2 – Шкала оценивания

Показатель оценки результатов обучения	Шкала оценивания
Пороговый уровень	60-72 баллов (удовлетворительно)
Продвинутый уровень	73-86 баллов (хорошо)
Высокий уровень	87-100 баллов (отлично)

5 Фонд оценочных средств.

Текущая аттестация и промежуточный контроль знаний магистрантов проводится по каждому календарному модулю (семестру) отдельно.

5.1 Фонд оценочных средств для текущего контроля

Текущий контроль используется для оперативного и регулярного управления учебной деятельностью (в том числе самостоятельной) магистрантов. В условиях рейтинговой системы контроля результаты текущего оценивания магистранта используются как показатель его текущего рейтинга. Текущий контроль успеваемости магистрантов включает в себя опрос и тестирование по всем темам курса и оценку правильности выполнение лабораторных работ. Полный перечень заданий для

лабораторных работ приведен в электронном обучающем курсе на платформе LMS MOODLE Красноярского.

5.1.1 Оценочное средство (опрос). Критерии оценивания.

Перечень вопросов (Модуль 1):

1. Понятие информационной безопасности. Основные составляющие. Важность проблемы.
2. Понятие угрозы. Наиболее распространенные угрозы. Классификация угроз.
3. Основные нормативные руководящие документы , касающиеся государственной тайны, нормативно-справочные документы.
4. Законодательный уровень информационной безопасности. Обзор зарубежного законодательства в области ИБ. Назначение и задачи в сфере обеспечения информационной безопасности.
5. Международные стандарты информационного обмена. Стандарт ISO/IEC15408.
6. Российские стандарты защищенности автоматизированных систем.
7. Основные положения теории информационной безопасности. Модели безопасности и их применение.
8. Информационная безопасность в условиях функционирования в России глобальных сетей.
9. Виды противников или "нарушителей". Понятия о видах вирусов Виды возможных нарушений информационной системы. Виды защиты.
10. Файловые вирусы.
11. Загрузочные вирусы.
12. Вирусы и операционные системы.
13. Методы и средства борьбы с вирусами.
14. Профилактика заражения вирусами компьютерных систем.
15. Защита информации от случайных угроз.
16. Дублирование информации. RAID - массивы
17. Повышение надежности компьютерных систем.
18. Обеспечение отказоустойчивости компьютерных систем.
19. Блокировка ошибочных операций.
20. Защита информации от традиционного шпионажа и диверсий.
21. Система охраны объектов компьютерных систем.
22. Организация работы с конфиденциальными информационными ресурсами.
23. Противодействие подслушиванию и наблюдению в оптическом диапазоне.
24. Средства борьбы с закладными подслушивающими устройствами.

Перечень вопросов (Модуль 2):

1. Защита от злоумышленных действий обслуживающего персонала и пользователей.
2. Средства защиты компьютеров. Программно аппаратные методы и средства ограничения доступа к компонентам компьютера. Типы несанкционированного доступа и условия работы средств защиты.
3. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем.
4. Защита от несанкционированного копирования программного обеспечения.
5. Методы криптографии
6. Основные понятия шифрования.
7. Методы шифрования с симметричным ключом.
8. Системы шифрования с открытым ключом.
9. Стандарты шифрования.
10. Промышленные программные средства Kerberos, PGP.
11. Методы и средства хранения ключевой информации. Анализ программных реализаций.
12. Защита от разрушающих программных воздействий.

13. Основные технологии построения защищенных ЭИС.
14. Системные вопросы защиты программ и данных.
15. Основные категории требований к средствам обеспечения информационной безопасности
16. Место информационной безопасности экономических систем в национальной безопасности страны
17. Безопасность платежных систем в среде Интернет.
18. Аналитические методы шифрования.
19. Программные закладки
20. Организационные методы защиты информации
21. Электронно-цифровая подпись.
22. Этапы враждебного воздействия
23. Кодирование информации
24. Методы враждебного воздействия

Критерии оценивания:

Баллы по рейтинго-модульной системе	Критерии оценивания
«4 балла»	Магистрантом дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, приводит собственные примеры по проблематике поставленного вопроса.
«3 балла»	Магистрантом дан развернутый ответ на поставленный вопрос, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе.
«2 балла»	Магистрантом дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа.
«0 баллов»	Магистрантом дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Магистрант не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.

5.1.2 Оценочное средство (лабораторные работы). Критерии оценивания

Полный перечень заданий для лабораторных работ приведен в электронном обучающем курсе на платформе LMS MOODLE Красноярского ГАУ.

Примерное задание для лабораторной работы

Восстановление зараженных файлов

Алгоритм выполнения работы.

Для восстановления документов Word и Excel достаточно сохранить пораженные файлы в текстовый формат RTF, содержащий практически всю информацию из первоначальных документов и не содержащий макросы.

Для этого выполните следующие действия.

1. В программе **WinWord** выберите пункты меню «**Файл**» – «**Сохранить как**» (Рис.1).
2. В открывшемся окне в поле «**Тип файла**» выберите «**Текст в формате RTF**»

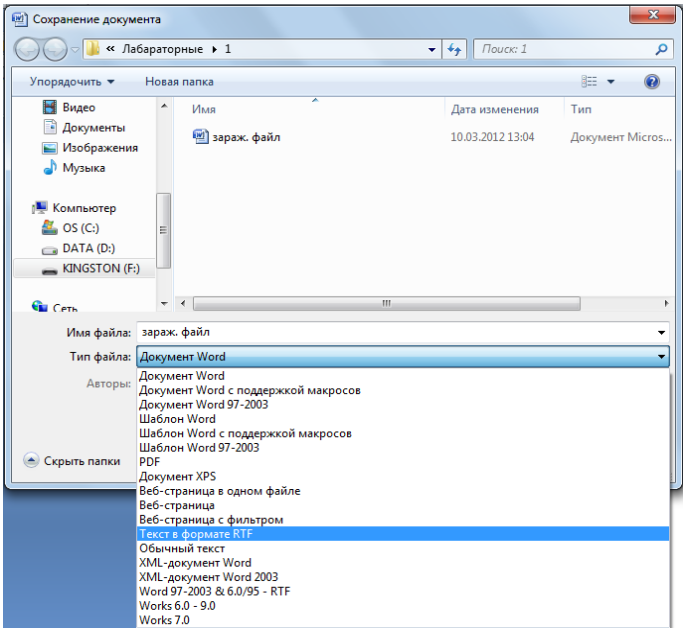

Рис.

3.Выберите команду **Сохранить**, при этом имя файла оставьте прежним.

4.В результате появится новый файл с именем существующего, но с другим расширением.

5.Далее закройте **WinWord** и удалите все зараженные Word-документы и файл-шаблон **NORMAL.DOT** в папке **WinWord**.

6.Запустите **WinWord** и восстановите документы из RTF-файлов в соответствующий формат файла (рис. 2) с расширением (.doc).

7.В результате этой процедуры вирус будет удален из системы, а практически вся информация останется без изменений.

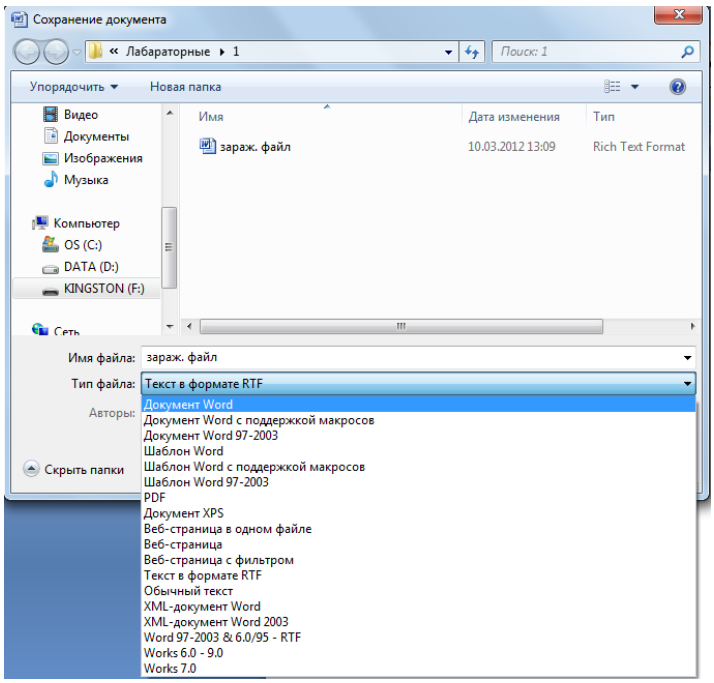

Рис.2

8.Для последующей защиты файлов от макровирусов включите защиту от запуска макросов.

9 Для этого в **WinWord** выберите последовательно пункты меню: **Сервис - Макрос - Безопасность (рис.3)**.

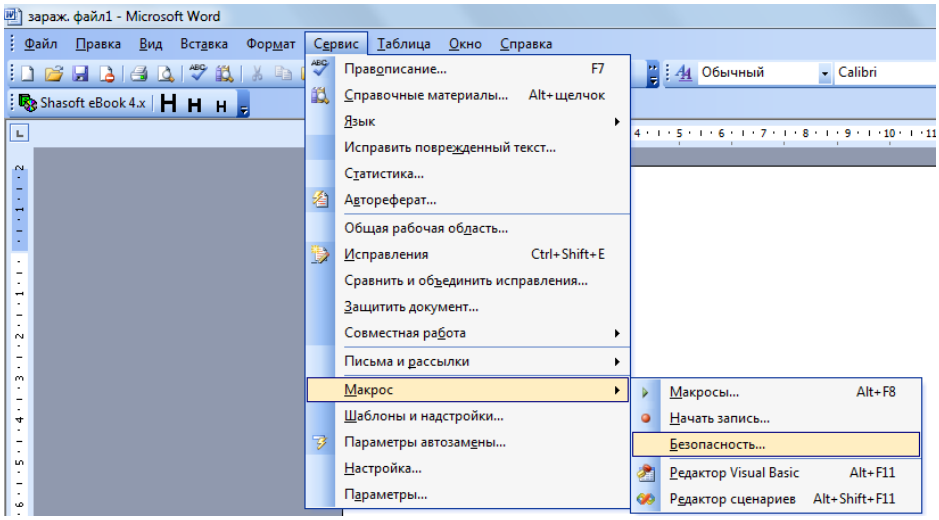

Рис.3

10.В открывшемся окне на закладке **Уровень безопасности** отметьте пункт **Высокая (рис.4).**

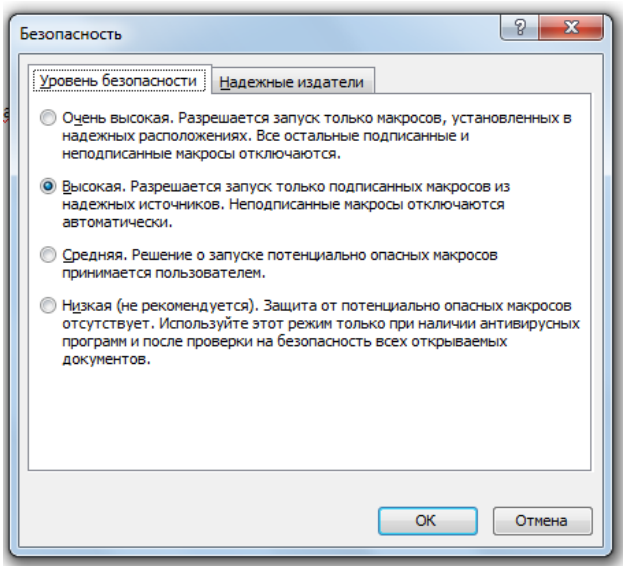

Рис. 4

1. Какие файлы заражают макровирусы?

Макровирусы заражают файлы – документы и электронные таблицы популярных офисных приложений.

2. Как просмотреть код макровируса?

Для анализа макровирусов необходимо получить текст их макросов. Для нешифрованных («не - стелс») вирусов это достигается при помощи меню Сервис/Макрос. Если же вирус шифрует свои макросы или использует «стелс»-приемы, то необходимо воспользоваться специальными утилитами просмотра макросов.

3. Как восстановить файл, зараженный макровирусом?

Для восстановления документов Word и Excel достаточно сохранить пораженные файлы в текстовый формат RTF, содержащий практически всю информацию из первоначальных документов и не содержащий макросы.

Полный перечень заданий для лабораторных работ приведен в электронном обучающем курсе на платформе LMS MOODLE Красноярского ГАУ.

Критерии оценивания:

За выполненные лабораторной работы магистрант получает баллы, количество которых рассчитывается по формуле:

$$N = \frac{P}{S} \times M$$,

где N – количество баллов, получаемых магистрантом, P – количество элементов работы, подлежащих оцениванию, которые магистрант выполнил правильно, S – общее количество элементов работы, подлежащих оцениванию, M – количество баллов за работу.

Итого за семестр в результате выполнения лабораторных работ магистрант может набрать максимум для модуля 1- 20 баллов. Шкала оценивания:

- 0 – 4 баллов – неудовлетворительно,
- 5 – 9 баллов – удовлетворительно,
- 10 – 14 баллов – хорошо,
- 15– 20 баллов – отлично.

5.1.3 Оценочное средство (Тестирование). Критерии оценивания.

Текущая аттестация проводится в форме тестирования по вопросам основных тем курса по каждому модулю в отдельности, за которое магистрант может получить до 15 баллов в модуле 1 и 15 баллов в модуле 2. Тест-билет содержит до 30 вопросов, время тестирования - 90 минут. Примеры тестовых заданий для каждого модуля приведены в приложении 1.

Критерии оценивания:

Критерии оценки тестирования (при количестве тестов - 30 в тест-билете)

Количество правильных ответов	%	Оценка	Баллы
25-30	85-100%	Отлично	15
21-24	70-85%	Хорошо	10
18-21	60-70%	удовлетворительно	5
< 18	<60%	неудовлетворительно	<5

Оценивание тестирования осуществляется по следующим критериям:

- магистрант, давший правильные ответы 85-100% (1-5 ошибок), получает максимальное количество баллов – 15.
- магистрант, давший правильные ответы в пределах 70-85% (6-10 ошибок), получает 10 баллов.
- магистрант, давший правильные ответы в пределах 60-70%, получает 5 баллов.
- магистрант, давший правильные ответы на менее чем 60% вопросов, не набирает баллов и приходит на контрольное тестирование снова.

Шкала оценивания:

- 0 - 3 баллов – неудовлетворительно,
- 4 – 7 баллов – удовлетворительно,
- 8 – 11 баллов – хорошо,
- 12 – 15 баллов – отлично.

Полный перечень тестовых заданий приведен в электронном обучающем курсе на платформе LMS MOODLE Красноярского ГАУ.

5.2 Фонд оценочных средств для промежуточного контроля

ФОС промежуточной аттестации обучающихся по дисциплине предназначен для оценки степени достижения запланированных результатов обучения по завершению изучения дисциплины в установленной учебным планом форме: зачет с оценкой – в 3 семестре.

В ходе текущего контроля проводится оценивание качества изучения и усвоения магистрантами учебного материала по разделам, темам, модулям (логически завершенной части учебного материала) в соответствии с требованиями программы.

5.2.1 Оценочное средство (итоговое тестирование(зачет с оценкой)). Критерии оценивания

Зачет с оценкой по дисциплине "Технологии защиты информации в компьютерных сетях " проводится в виде тестирования по вопросам основных тем курса, за которое магистрант может получить до 20 баллов в 3 семестре. Тест-билет содержит до 30 вопросов, время тестирования - 90 минут. Примеры тестовых заданий приведены в приложении 2.

Критерии оценивания:

Критерии оценки итогового тестирования (при количестве тестов - 30 в тест-билете)

Количество правильных ответов	%	Оценка	Баллы
25-30	85-100%	Отлично	20
21-24	70-85%	Хорошо	14
18-21	60-70%	удовлетворительно	12
< 18	<60%	неудовлетворительно	<12

Оценивание зачетного тестирования осуществляется по следующим критериям:

- магистрант, давший правильные ответы 85-100% (1-5 ошибок), получает максимальное количество баллов – 20.
- магистрант, давший правильные ответы в пределах 70-85% (6-10 ошибок), получает 14 баллов.
- магистрант, давший правильные ответы в пределах 60-70%, получает 12 баллов.
- магистрант, давший правильные ответы на менее чем 60% вопросов, не набирает баллов и приходит на контрольное тестирование снова.

Баллы, полученные на зачетном тестировании суммируются с баллами, полученными в течение семестра на текущей аттестации и выводится итоговая оценка:

- 60 – 72 баллов – оценка «удовлетворительно».
- 73 – 86 баллов – оценка «хорошо».
- 87 – 100 баллов – оценка «отлично».

Обучающийся, не сдавший зачет, приходит на пересдачу в сроки в соответствии с графиком ликвидации академических задолженностей: http://www.kgau.ru/new/news/news/2017/grafik_lz.pdf.

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2025. — 349 с. — (Высшее образование). — ISBN 978-5-534-19762-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561077
2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебник для вузов / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 352 с. — (Высшее образование). — ISBN 978-5-534-19386-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/580669

6.2 Дополнительная литература

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2025. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562070

6.3 Методические указания, рекомендации и другие материалы к занятиям

Титовский С.Н., Титовская Н.В.Информационная безопасность. Электронный обучающий ресурс. http://e.kgau.ru/course/view.php?id=1051

6.4 Программное обеспечение

Лицензионное ПО Красноярского ГАУ

1. Операционная система Astra Linux (лицензия № 192400033-alse-1.7-client-base_orel-x86_64-0-12913 от 28.08.2023).
2. Офисный пакет приложений Libre Office входит в комплект поставки Astra Linux.
3. Офисный пакет приложений Мой Офис (лицензия № ПР0000-35377 от 24.07.2024).
4. Moodle 3.5.6a (договор № 969.2 от 17.04.2020).

Свободно-распространяемое ПО

1. Wireshark,
2. Oracle VM Virtual Box,
3. Graphical Network Simulator-3

6.5 Интернет ресурсы, электронные библиотечные системы

Интернет-ресурсы

1. Информационная безопасность. Электронный обучающий ресурс https://e.kgau.ru/course/view.php?id=1051 (Moodle)
2. Национальный Открытый Университет «ИНТУИТ» https://intuit.ru/
3. Портал CIT Forum http://citforum.ru/
4. Форум программистов и сисадминов Киберфорум https://www.cyberforum.ru/
5. Информационно-аналитическая система «Статистика» http://www.ias-stat.ru/

Электронные библиотечные системы

1. Каталог библиотеки Красноярского ГАУ -- www.kgau.ru/new/biblioteka/ ;
2. ЭБС Издательства «Лань», адрес сайта: http://e.lanbook.com (договор № 45 от 10.03.2021); (договор №13/4-21 от 03.09.2021); (договор №21/5-22 от 05.03.2022); (договор №1 от 19.03.2023); (договор №2 от 19.03.2023); (Договор №1/14-24 от 29.02.2024); (№2/14-24 от 04.03.2024); (№1/14-25 от 17.02.2025); (№2/14-25 от 17.02.2025).
3. ЭБС издательства «Юрайт», адрес сайта https://urait.ru/ (договор №10/4-21 от 31.03. 2021); (договор №12/4-21 от 16.06. 2021); (договор №5293 от 23.05.2022); (договор №5857 от 16.05.2023); (договор №36/4-24 от 15.05.2024, договор №3-14-25 от 25.06.25).
4. ЭБС Руконт, адрес сайта https://lib.rucont.ru/ (Издательство Колосс «Сельское хозяйство», научные монографии) (договор №18/4-23 от 01.03.2023); (№32/4-23 от 02.10.2023); (№16/4-24 от 20.02.2024); (№б/4-25 от 24.02.2025)
5. Коллекция электронных изданий Сибирского федерального университета (договор о сотрудничестве № 200/10-20 от 25.09.2020 ФГАОУ ВО «Сибирский федеральный университет»)
6. Национальная электронная библиотека https://rusneb.ru/ (договор №101/НЭБ/2276 о предоставлении доступа к от 06.06.2017 ФГБУ «РГБ»)
7. Электронная библиотечная система «ИРБИС64+» - http://5.159.97.194:8080/cgi-bin/irbis64r_plus/cgiirbis_64_ft.exe?C21COM=F&I21DBN=IBIS_FULLTEXT&P21DBN=IBIS&Z21ID=&S21CNR=5
8. Электронный каталог Государственной универсальной научной бибилиотеки Красноярского края - https://www.kraslib.ru/
9. Научная электронная библиотека «КиберЛенинка». https://cyberleninka.ru
10. Lens.org https://www.lens.org
11. Dimensions https://app.dimensions.ai
12. Bielefeld Academic Search Engine https://www.base-search.net
13. Semantic Scholar https://www.semanticscholar.org
14. OpenAlex https://openalex.org
15. Wiley https://onlinelibrary.wiley.com/

16. Национальный агрегатор открытых репозиториев https://www.openrepository.ru/

Информационно-справочные системы

1. Информационно-правовой портал «Гарант». http://www.garant.ru/
2. Справочно-правовая система «Консультант +» https://www.consultant.ru (договор №20059900202 об информационной поддержке от 02.03.2015 ООО Информационный центр «Искра»;

Профессиональные базы данных

1. Коллективный блог по информационным технологиям, бизнесу и интернету. https://habr.com/ru/
2. OpenNet. Адрес ресурса: http://www.opennet.ru/

Приложение 1

Таблица – Тип тестового задания

Тип задания	Наименование
1	Задания закрытого типа на установление соответствия
2	Задания закрытого типа на установление последовательности
3	Задания комбинированного типа, предполагающие выбор одного правильного ответа из предложенных
4	Задания комбинированного типа, предполагающие выбор нескольких ответов из предложенных
5	Задания открытого типа, в том числе с развёрнутым ответом

Примеры тестовых заданий (модуль 1)

Тип задания	Задание	Правильный ответ
3	1 Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. К методам несанкционированного доступа к ресурсам системы рассылки новостей USENET относится: 1. паразитный сетевой трафик; 2. метод заочного воздействия на объекты; 3. использование люков в интерфейсе CGI; 4. использование постоянно поступающей информации.	4
3	2. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Программная закладка (ПЗ) записывается в ПЗУ, в системное или прикладное обеспечение и сохраняет вводимую, выводимую информацию в скрытую область памяти локального или удаленного компьютера. Этот метод воздействия программных закладок на компьютер называется: 1. «Перехват» 2. «Искажение» 3. «Наблюдатель» 4. «Компрометация».	1
3	3. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. К методам несанкционированного доступа к клиентскому программному обеспечению www относится: 1. передача бессмысленных огромных файлов по низкоскоростным каналам; 2. перегрузка серверов сети незавершенными процессами установки соединений; 3. метод несанкционированного доступа, ориентированный на серверы www. 4. использование управляющих сообщений;	3
3	4. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. К методам создания скрытых каналов передачи данных относится: 1. передача программ, создающих скрытый канал обмена сквозь firewall через порт 80. 2. получение привилегированного доступа к потоку новостей; 3. создание специального сервера www; 4. проверка текущих задач пользователя;	1
5	5. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки.	нелицензионного

	Наиболее распространенной угрозой информационной безопасности корпоративной системы является покупка _____ программного обеспечения.	
5	6. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Секретность закрытого сообщения определяется секретностью ключа – называется принципом _____.	Кирхгофа
5	7. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Используя асинхронную природу ОС компьютерную систему, заставляют работать в сложных условиях, из-за чего работа нарушается. Данная ситуация используется для внесения изменений в ОС, при чем эти изменения не будут заметны. Этот метод называется _____ атака.	асинхронная
5	8. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Программа, заражающая другие программы, путем включения в них своей модифицированной копии, при чем последняя имеет способность к дальнейшему распространению, называется _____.	вирус
1	9. Прочитайте текст и установите соответствие между методами вредоносных воздействий и их реализацией 1. Метод снижения эффективности работы сети на уровне транспортных и коммуникационных протоколов 2. Метод несанкционированного доступа к ресурсам системы рассылки новостей USENET 3. Метод несанкционированного доступа к клиентскому программному обеспечению WWW 4. Метод несанкционированного доступа к электронной почте А) создание скрытых каналов передачи данных Б) несанкционированное использование SMTP-сервера В) использование люков в интерфейсе CGI Г) удаление ранее отправленного в телеконференцию сообщения	1-А, 2-Г, 3-В, 4-Б
1	10 Прочитайте текст и установите соответствие между разновидностями вирусов и их воздействием 1. файловый нерезидентный вирус 2. файловый резидентный вирус 3. бутовый вирус 4. гибридный А. заражает не только исполняемые файлы, находящиеся во внешней памяти, но и оперативную память Б) целиком размещается в исполняемом файле, в связи с чем он активизируется только в случае активизации вирусоносителя, а по выполнении необходимых действий возвращает управление самой программе В) инфицируют как файлы, так бут-сектора Г)инфицируют загрузочный (бут-сектор) магнитного носителя;	1-Б, 2-А, 3-Г, 4 –В
3	11. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. К методам несанкционированного доступа к электронной почте относится: 1. несанкционированное использование SMTP-сервера. 2. получение списка пользователей сервера 3. создание паразитного трафика	1

	4. засорение новостных каналов устаревшей информацией	
3	12. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. По времени пребывания программных закладок в оперативной памяти можно выделить следующие типы закладок: 1. постоянные; 2. временные; 3. краткосрочные; 4. резидентные.	4
3	13. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Эта программа в процессе своего функционирования выполняет применительно к каждому исполняемому файлу сравнение его текущих характеристик с аналогичными характеристиками, полученными в ходе предшествующего просмотра: 1. детектор; 2. вакцина; 3. монитор; 4. ревизор.	4
4	14. Прочитайте текст, выберите все правильные варианты ответа и запишите аргументы, обосновывающие выбор ответа. Свойство резидентности предполагает выполнение вирусом на этапе загрузки двух действий 1. закрепление в памяти. 2. перехват системных функций. 3. поглашение системных ресурсов 4. подключение к линиям связи	1, 2
5	15. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Гарантия того, что секретные данные будут доступны только авторизованным пользователям, которым этот доступ разрешен называется _____.	конфиденциальность
5	16. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. К методам снижения эффективности работы сети на уровне транспортных и коммуникационных протоколов относится _____ пропускной способности каналов передачи данных.	деградация
5	17. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. _____ независимая сеть передачи данных, лишь организационно входящая в состав internet и использующая нижние уровни протоколов TCP/IP.	usenet
3	18. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. При подключении к серверу рассылки новостей система сообщает об используемой версии сервера, а также о том, разрешен ли режим загрузки внешних сообщений и имя системы, на которой запущен данный сервер. Это принцип действия метода: 1) восстановления структуры сети рассылки новостей 2) идентификационной строки сервера рассылки новостей 3) подмены документов серверов нецензурными изображениями 4)перехвата электронной почты	2
1	19. Прочитайте текст и установите соответствие между методами вредоносных воздействий и их названием	1-В, 2-Б, 3-А

	1. Метод, при котором происходит подключение к линиям связи и перехват работы после окончания сеанса законного пользователя: 2. Метод при котором происходит создание условий, когда законный пользователь осуществляет связь с нелегальным терминалом, будучи уверенным, в том, что он работает с необходимым ему абонентом называется: 3. Используя асинхронную природу ОС компьютерную систему, заставляют работать в сложных условиях, из-за чего работа нарушается. Данная ситуация используется для внесения изменений в ОС, при чем эти изменения не будут заметны. Этот метод называется:	А) асинхронная атака Б) «мистификация» В) «за хвост»	
1	20. Прочитайте текст и установите соответствие между разновидностями вредоносных воздействий и реализующими их методами		1-В, 2-В, 3-А
	1. Методы несанкционированного доступа ориентированные на нештатное использование программ- браузеров HTML-страниц WWW, а также на применение программ, расширяющих функциональные возможности браузеров для решения не свойственных им задач- это: 2. К методам снижения эффективности работы сети на уровне транспортных и коммуникационных протоколов относится: 3. К методам несанкционированного доступа к ресурсам системы рассылки новостей USENET относится:	А) вскрытие структуры сети и основных информационных каналов по анализу распространения новостей USENET Б) Методы доступа, основанные на отдельных элементах протокола NNTP В) методы несанкционированного доступа к клиентскому программному обеспечению WWW	
3	21. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Какой орган лицензирует деятельность по защите информации? 1. Министерство по сертификации 2. МВД 3. Федеральная служба по техническому и экспортному контролю (ФСТЭК России). 4. Министерство обороны		3
3	22. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Антивирусы обеспечивающие выявление вирусов посредством просмотра исполняемых файлов поиска так называемых сигнатур- это: 1. детекторы. 2. фаги; 3. вакцины; 4. мониторы;		1
3	23. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Резидентная программа, обеспечивающая перехват потенциально опасных прерываний, характерных для вирусов, и запрашивающая у пользователей подтверждение на выполнение операций, следующих за прерыванием - это: 1. прививка; 2. ревизор; 3. вакцина; 4. монитор.		4

4	24. Прочитайте текст, выберите все правильные варианты ответа и запишите аргументы, обосновывающие выбор ответа. По способу инфицирования жертвы вирусы можно разделить на классы 1. вирусы, которые не внедряют свой код непосредственно в программный файл, а изменяют имя файла и создают код старым именем новый, содержащий тело вируса. 2. Вирусы, внедряющиеся непосредственно в файлы жертвы. 3. Вирусы, внедряющиеся в системную среду ОС	1,2
5	25. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Обеспечение субъекту возможности ознакомления с информацией и ее обработки, в частности, копирования, модификации или уничтожения информации называется _____-к информации..	доступ
5	26. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. _____ - это гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.	целостность
2	27. Прочитайте текст и установите последовательность порядка Перечислите последовательность цикла жизни вируса: 1. проявление 2. период репликации 3. инкубационный период 4. внедрение	4,3,2,1
5	28. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Макропрограммы и файлы документов современных систем обработки информации. такие вирусы называются __ _____	макровирусами
1	29. Прочитайте текст и установите соответствие между разновидностями ПО защиты от вредоносных воздействий и их категориями 1. Антивирусы обеспечивающие выявление вирусов посредством просмотра исполняемых файлов поиска так называемых сигнатур- это: 2. Резидентная программа, обеспечивающая перехват потенциально опасных прерываний, характерных для вирусов, и запрашивающая у пользователей подтверждение на выполнение операций, следующих за прерыванием - это: 3. Эта программа в процессе своего функционирования выполняет применительно к каждому исполняемому файлу сравнение его текущих характеристик с аналогичными характеристиками, полученными в ходе предшествующего просмотра это: 4. Антивирусы выполняющие функции, свойственные детекторам, но кроме того, излечивают инфицированные программы посредством «выкусывания» вирусов из них- это: А)монитор Б) детекторы В) фаги Г) ревизор	1-Б, 2-А, 3-Г, 4-В
4	30. Прочитайте текст, выберите все правильные варианты ответа и запишите аргументы, обосновывающие выбор ответа. Выберите все ***неверные*** варианты ответов. Закон «Об информации, информатизации и защите информации» выделяет следующие цели: 1. Предотвращение утечки, хищения, утраты, подделки; 2. Предотвращение угроз безопасности личности, угроз государству;	3, 4

	3. Защита конституционных прав гражданина на сохранение личной тайны. 4. Право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.	

Примеры тестовых заданий (модуль 2)

Тип задания	Задание	Правильный ответ
3	1. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Идентификация – это: 1. защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб владельцам или пользователям информации; 2. целенаправленное регулярное применение в автоматизированных системах средств и методов защиты информации, а также осуществление комплекса мероприятий с целью поддержания заданного уровня защищенности информации по всей совокупности показателей и условий, являющихся существенно значимыми с точки зрения обеспечения безопасности информации; 3. гарантия того, что секретные данные будут доступны только пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными); 4. присвоение субъектам и объектам доступа уникального идентификатора в виде номера, шифра, кода и т.п. с целью получения доступа к информации.	4
3	2. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Целенаправленное регулярное применение в автоматизированных системах средств и методов защиты информации, а также осуществление комплекса мероприятий с целью поддержания заданного уровня защищенности информации по всей совокупности показателей и условий, являющихся существенно значимыми с точки зрения обеспечения безопасности информации– это: 1. Аутентификация; 2. Комплексная защита информации. 3. Информационная безопасность; 4. Доступ к информации;	2
3	3. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. К методам снижения эффективности работы сети на уровне транспортных и коммуникационных протоколов относится: 1. выведение из строя серверов сети internet. 2. использование управляющих сообщений 3. создание и удаление новостных каналов 4. переполнение браузера с разрушением области кодов	1
5	4. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб	информационная безопасность

	владельцам или пользователям информации называется _____ _____.	
5	5. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах ЭЦП с использованием средств ЭЦП называется _____ ключом ЭЦП;	закрытым
5	6. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Проверка подлинности партнеров по общению и источников данных (предотвращает маскарад, повтор предыдущего сеанса) называется _____.	аутентификация
5	7. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Программная закладка (ПЗ) записывается в ПЗУ, в системное или прикладное обеспечение и сохраняет вводимую, выводимую информацию в скрытую область памяти локального или удаленного компьютера. Этот метод воздействия программных закладок на компьютер называется _____.	перехват
4	8. Прочитайте текст, выберите все правильные варианты ответа и запишите аргументы, обосновывающие выбор ответа. По способу поиска жертвы вирусы можно разделить на классы: 1. осуществляющие активный поиск с использованием функций операционной системы. 2. реализующий первостепенный поиск в загрузочной области жесткого диска 3. реализующие пассивный механизм поиска.	1, 3
1	9. Прочитайте текст и установите соответствие между методами вредоносных воздействий и их реализацией 1. Метод снижения эффективности работы сети на уровне транспортных и коммуникационных протоколов 2. Метод несанкционированного доступа к электронной почте 3. Метод несанкционированного доступа к ресурсам системы рассылки новостей USENET 4. Метод несанкционированного доступа к клиентскому программному обеспечению www А) переполнение буфера с разрушением области кодов Б) выведение из строя серверов сети internet В) перехват электронной почты Г) использование постоянно поступающей информации	1-Б, 2-В, 3-Г, 4-А
1	10. Прочитайте текст и установите соответствие между разновидностями вирусов и их воздействием 1. файловый нерезидентный вирус 2. файловый резидентный вирус 3. бутовый вирус 4. гибридный А. заражает не только исполняемые файлы, находящиеся во внешней памяти, но и оперативную память Б) целиком размещается в исполняемом файле, в связи с чем он активизируется только в случае активизации вирусоносителя, а по выполнении необходимых действий возвращает управление самой программе В) инфицируют как файлы, так бут-сектора	1-Б, 2-А, 3-Г, 4 –В

		Г)инфицируют загрузочный (бут-сектор) магнитного носителя;	
3	11. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Гарантия того, что секретные данные будут доступны только пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными) – это: 1. Идентификация; 2. Угроза; 3. Целостность; 4. Конфиденциальность.		4
3	12. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. В какой стране была создана Комиссия по защите важных информационных ресурсов? 1. Россия; 2. Италия; 3. США. 4. Япония;		3
3	13. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Первый компьютерный вирус был написан в 1. 1953; 2. 1971. 3. 1990; 4. 1951;		2
5	14. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. «_____- соответствует периоду, когда вирус хранится на диске совместно с объектом, в который он внедрен».		хранение
5	15. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. _____ _____ - это специально скрытно внедренная в защитную систему программа, позволяющая злоумышленнику путем модификации свойств системы защиты осуществлять несанкционированный доступ к тем или иным ресурсам системы.		программная закладка
5	16. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. _____ - это гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.		целостность
5	17. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. _____ - специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении требований и условий, выданное юридическому лицу или индивидуальному предпринимателю.		лицензия
5	18. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Уникальная последовательность символов, соответствующая закрытому ключу ЭЦП, доступная любому пользователю ИС и предназначенная для подтверждения подлинности ЭЦП в электронном документе называется _____ ключом ЭЦП;		Открытым

<table>
<tr><td>1</td><td colspan="2">19. Прочитайте текст и установите соответствие между терминами и их определениями</td><td>1 –Г ,2–Д, 3–Б, 4–А, 5–В</td></tr>
<tr><td></td><td>1. Доступность
2. Атака
3. Защита информации
4. Угроза
5. Аутентификация</td><td>А) Любое действие, направленное на нарушение конфиденциальности, целостности и доступности информации, а также нелегальное использование других ресурсов информационной системы
Б) Комплекс мероприятий, направленных на обеспечение ИБ
Д) Реализованная угроза
Г) Гарантия того, что авторизованные пользователи всегда получат доступ к данным
В) Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы</td><td></td></tr>
<tr><td>1</td><td colspan="2">20. Прочитайте текст и установите соответствие между терминами и их определениями</td><td>1–Д, 2–В, 3–А, 4–Б, 5–Г</td></tr>
<tr><td></td><td>1. Целостность
2. Идентификация
3. Угроза
4. Конфиденциальность
5. Аутентификация</td><td>А) Любое действие, направленное на нарушение конфиденциальности, целостности и доступности информации, а также нелегальное использование других ресурсов информационной системы
Б) Гарантия того, что секретные данные будут доступны только пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными)
Д) Гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные
Г) Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы
В) Присвоение субъектам и объектам доступа уникального идентификатора в виде номера, шифра, кода и т.п. с целью получения доступа к информаци</td><td></td></tr>
<tr><td>3</td><td colspan="2">21. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа.
Физическое или функциональное повреждение устройств и компонентов сети, что приводит к нарушению их работы и, как следствие, к сбоям в передаче и обработке данных это
1. Искажение, уменьшение объема,
2. Перекодировка информации,
3. Техническое вмешательство, выведение из строя оборудования сети,
4. Потеря, искажение, утечка информации.</td><td>3</td></tr>
<tr><td>3</td><td colspan="2">22. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа.
Принципом информационной безопасности является принцип недопущения:</td><td>1</td></tr>
</table>

	1. Неоправданных ограничений при работе в сети (системе). 2. Рисков безопасности сети, системы; 3. Презумпции секретности;	
3	23. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные – это: 1. Идентификация 2. Угроза 3. Целостность 4. Конфиденциальность	3
3	24. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. К основным типам средств воздействия на компьютерную сеть относится: 1. Компьютерный сбой 2. Логические закладки («мины») 3. Аварийное отключение питания	2
3	25. Прочитайте текст, выберите все правильные варианты ответа и запишите аргументы, обосновывающие выбор ответа. .К методам выведения из строя серверов сети internet относится: 1. перехват электронной почты; 2. получение списка пользователей сервера. 3. пересылка файлов, которые приводят к краху программ-браузеров. 4. перехват номеров кредитных карточек.	2
5	26. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Программа, заражающая другие программы, путем включения в них своей модифицированной копии, причем последняя имеет способность к дальнейшему распространению, называется _____.	вирус
5	27. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Программа, специально предназначенная для перехвата паролей, называется _____ _____. .	захватчик паролей
2	28. Прочитайте текст и установите последовательность порядка Укажите все этапы жизненного цикла вируса в порядке выполнения. 1. поиск жертвы. 2. заражение найденной жертвы в 3. выполнение деструктивных функций 4. загрузка вируса в память 5. выполнение паразитологического сценария систем	4, 1, 2, 3
1	29. Прочитайте текст и установите соответствие между способами внедрения программных закладок и реализацией этих способов. 1. Внесение программных дефектов вирусного типа 2. Несанкционированный доступ к ресурсам компьютерной системы 3. Несанкционированное вмешательство в процесс обмена сообщениями между узлами связи сети ЛВС А) Осуществляется путем передачи следующих сообщений: • разрушающих; • искажающих; • имитирующих; хаотических Б) Внедрение возможно на всех участках жизненного цикла ПО: • эскизного и технического проектирования;	1-Б, 2-В, 3-А

<table>
<tr><td></td><td></td><td>• рабочего проектирования;
• внедрения; эксплуатации, включая сопровождение и модернизацию
В) Действия по использованию, изменению и уничтожению используемых модулей и массивов данных, производимые субъектом, не имеющим права на такие действия</td><td></td></tr>
<tr><td rowspan="2">1</td><td colspan="2">30. Прочитайте текст и установите соответствие между методами вредоносных воздействий и их реализацией</td><td rowspan="2">1-А, 2-Г, 3-В, 4-Б</td></tr>
<tr><td>1. Метод снижения эффективности работы сети на уровне транспортных и коммуникационных протоколов
2. Метод несанкционированного доступа к ресурсам системы рассылки новостей USENET
3. Метод несанкционированного доступа к клиентскому программному обеспечению WWW
4. Метод несанкционированного доступа к электронной почте</td><td>А) создание скрытых каналов передачи данных
Б) несанкционированное использование SMTP-сервера
В) использование люков в интерфейсе CGI
Г) удаление ранее отправленного в телеконференцию сообщения ;</td></tr>
</table>

Приложение 2

Таблица – Тип тестового задания

Тип задания	Наименование
1	Задания закрытого типа на установление соответствия
2	Задания закрытого типа на установление последовательности
3	Задания комбинированного типа, предполагающие выбор одного правильного ответа из предложенных
4	Задания комбинированного типа, предполагающие выбор нескольких ответов из предложенных
5	Задания открытого типа, в том числе с развёрнутым ответом

Примеры тестовых вопросов/заданий для зачета с оценкой

Тип задания	Задание	Правильный ответ
3	1. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Идентификация – это: 1. защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб владельцам или пользователям информации; 2. целенаправленное регулярное применение в автоматизированных системах средств и методов защиты информации, а также осуществление комплекса мероприятий с целью поддержания заданного уровня защищенности информации по всей совокупности показателей и условий, являющихся существенно значимыми с точки зрения обеспечения безопасности информации; 3. гарантия того, что секретные данные будут доступны только пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными); 4. присвоение субъектам и объектам доступа уникального идентификатора в виде номера, шифра, кода и т.п. с целью получения доступа к информации.	4
3	2. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Целенаправленное регулярное применение в автоматизированных системах средств и методов защиты информации, а также осуществление комплекса мероприятий с целью поддержания заданного уровня защищенности информации по всей совокупности показателей и условий, являющихся существенно значимыми с точки зрения обеспечения безопасности информации– это: 1. Аутентификация; 2. Комплексная защита информации. 3. Информационная безопасность; 4. Доступ к информации;	2
3	3. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. К методам снижения эффективности работы сети на уровне транспортных и коммуникационных протоколов относится: 1. выведение из строя серверов сети internet. 2. использование управляющих сообщений 3. создание и удаление новостных каналов	1

	4. переполнение браузера с разрушением области кодов	
5	4. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб владельцам или пользователям информации называется _____ _____.	информационная безопасность
5	5. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах ЭЦП с использованием средств ЭЦП называется _____ ключом ЭЦП;	закрытым
5	6. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Проверка подлинности партнеров по общению и источников данных (предотвращает маскарад, повтор предыдущего сеанса) называется _____.	аутентификация
5	7. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Программная закладка (ПЗ) записывается в ПЗУ, в системное или прикладное обеспечение и сохраняет вводимую, выводимую информацию в скрытую область памяти локального или удаленного компьютера. Этот метод воздействия программных закладок на компьютер называется _____.	перехват
4	8. Прочитайте текст, выберите все правильные варианты ответа и запишите аргументы, обосновывающие выбор ответа. По способу поиска жертвы вирусы можно разделить на классы: 1. осуществляющие активный поиск с использованием функций операционной системы. 2. реализующий первостепенный поиск в загрузочной области жесткого диска 3. реализующие пассивный механизм поиска.	1, 3
1	9. Прочитайте текст и установите соответствие между методами вредоносных воздействий и их реализацией 1. Метод снижения эффективности работы сети на уровне транспортных и коммуникационных протоколов 2. Метод несанкционированного доступа к электронной почте 3. Метод несанкционированного доступа к ресурсам системы рассылки новостей USENET 4. Метод несанкционированного доступа к клиентскому программному обеспечению www А) переполнение буфера с разрушением области кодов Б) выведение из строя серверов сети internet В) перехват электронной почты Г) использование постоянно поступающей информации	1-Б, 2-В, 3-Г, 4-А
1	10. Прочитайте текст и установите соответствие между разновидностями вирусов и их воздействием 1. файловый нерезидентный вирус 2. файловый резидентный вирус 3. бутовый вирус А. заражает не только исполняемые файлы, находящиеся во внешней памяти, но и оперативную память Б) целиком размещается в исполняемом файле, в связи с чем он	1-Б, 2-А, 3-Г, 4 –В

	4. гибридный	активизируется только в случае активизации вирусоносителя, а по выполнении необходимых действий возвращает управление самой программе В) инфицируют как файлы, так бут-сектора Г)инфицируют загрузочный (бут-сектор) магнитного носителя;	
3	11. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Гарантия того, что секретные данные будут доступны только пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными) – это: 1. Идентификация; 2. Угроза; 3. Целостность; 4. Конфиденциальность.		4
3	12. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. В какой стране была создана Комиссия по защите важных информационных ресурсов? 1. Россия; 2. Италия; 3. США. 4. Япония;		3
3	13. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Первый компьютерный вирус был написан в 1. 1953; 2. 1971. 3. 1990; 4. 1951;		2
5	14. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. «_____- соответствует периоду, когда вирус хранится на диске совместно с объектом, в который он внедрен».		хранение
5	15. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. _____ _____ - это специально скрытно внедренная в защитную систему программа, позволяющая злоумышленнику путем модификации свойств системы защиты осуществлять несанкционированный доступ к тем или иным ресурсам системы.		программная закладка
5	16. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. _____ - это гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.		целостность
5	17. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. _____ - специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении требований и условий, выданное юридическому лицу или индивидуальному предпринимателю.		лицензия

<table>
<tr><td>5</td><td colspan="2">18. Внимательно прочитать текст задания и понять суть вопроса.
Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки.
Уникальная последовательность символов, соответствующая закрытому ключу ЭЦП, доступная любому пользователю ИС и предназначенная для подтверждения подлинности ЭЦП в электронном документе называется _____ ключом ЭЦП;</td><td>Открытым</td></tr>
<tr><td rowspan="2">1</td><td colspan="2">19. Прочитайте текст и установите соответствие между терминами и их определениями</td><td rowspan="2">1 –Г ,2–Д, 3–Б, 4–А, 5–В</td></tr>
<tr><td>1. Доступность
2. Атака
3. Защита информации
4. Угроза
5. Аутентификация</td><td>А) Любое действие, направленное на нарушение конфиденциальности, целостности и доступности информации, а также нелегальное использование других ресурсов информационной системы
Б) Комплекс мероприятий, направленных на обеспечение ИБ
Д) Реализованная угроза
Г) Гарантия того, что авторизованные пользователи всегда получат доступ к данным
В) Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы</td></tr>
<tr><td rowspan="2">1</td><td colspan="2">20. Прочитайте текст и установите соответствие между терминами и их определениями</td><td rowspan="2">1–Д, 2–В, 3–А, 4–Б, 5–Г</td></tr>
<tr><td>1. Целостность
2. Идентификация
3. Угроза
4. Конфиденциальность
5. Аутентификация</td><td>А) Любое действие, направленное на нарушение конфиденциальности, целостности и доступности информации, а также нелегальное использование других ресурсов информационной системы
Б) Гарантия того, что секретные данные будут доступны только пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными)
Д) Гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные
Г) Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы
В) Присвоение субъектам и объектам доступа уникального идентификатора в виде номера, шифра, кода и т.п. с целью получения доступа к информаци</td></tr>
<tr><td>3</td><td colspan="2">21. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа.
Физическое или функциональное повреждение устройств и компонентов сети, что приводит к нарушению их работы и, как следствие, к сбоям в передаче и обработке данных это
1. Искажение, уменьшение объема,
2. Перекодировка информации,</td><td>3</td></tr>
</table>

	3. Техническое вмешательство, выведение из строя оборудования сети, 4. Потеря, искажение, утечка информации.	
3	22. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Принципом информационной безопасности является принцип недопущения: 1. Неоправданных ограничений при работе в сети (системе). 2. Рисков безопасности сети, системы; 3. Презумпции секретности;	1
3	23. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные – это: 1. Идентификация 2. Угроза 3. Целостность 4. Конфиденциальность	3
3	24. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. К основным типам средств воздействия на компьютерную сеть относится: 1. Компьютерный сбой 2. Логические закладки («мины») 3. Аварийное отключение питания	2
3	25. Прочитайте текст, выберите все правильные варианты ответа и запишите аргументы, обосновывающие выбор ответа. .К методам выведения из строя серверов сети internet относится: 1. перехват электронной почты; 2. получение списка пользователей сервера. 3. пересылка файлов, которые приводят к краху программ-браузеров. 4. перехват номеров кредитных карточек.	2
5	26. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Программа, заражающая другие программы, путем включения в них своей модифицированной копии, причем последняя имеет способность к дальнейшему распространению, называется _____.	вирус
5	27. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Программа, специально предназначенная для перехвата паролей, называется _____ _____. .	захватчик паролей
2	28. Прочитайте текст и установите последовательность порядка Укажите все этапы жизненного цикла вируса в порядке выполнения. 1. поиск жертвы. 2. заражение найденной жертвы в 3. выполнение деструктивных функций 4. загрузка вируса в память 5. выполнение паразитологического сценария систем	4, 1, 2, 3
1	29. Прочитайте текст и установите соответствие между способами внедрения программных закладок и реализацией этих способов.	1-Б, 2-В, 3-А
	1. Внесение программных дефектов вирусного типа 2. Несанкционированный доступ к ресурсам	А) Осуществляется путем передачи следующих сообщений: • разрушающих;

	компьютерной системы 3. Несанкционированное вмешательство в процесс обмена сообщениями между узлами связи сети ЛВС	• искажающих; • имитирующих; хаотических Б) Внедрение возможно на всех участках жизненного цикла ПО: • эскизного и технического проектирования; • рабочего проектирования; • внедрения; эксплуатации, включая сопровождение и модернизацию В) Действия по использованию, изменению и уничтожению используемых модулей и массивов данных, производимые субъектом, не имеющим права на такие действия	
1	30. Прочитайте текст и установите соответствие между методами вредоносных воздействий и их реализацией		1-А, 2-Г, 3-В, 4-Б
	1. Метод снижения эффективности работы сети на уровне транспортных и коммуникационных протоколов 2. Метод несанкционированного доступа к ресурсам системы рассылки новостей USENET 3. Метод несанкционированного доступа к клиентскому программному обеспечению WWW 4. Метод несанкционированного доступа к электронной почте	А) создание скрытых каналов передачи данных Б) несанкционированное использование SMTP-сервера В) использование люков в интерфейсе CGI Г) удаление ранее отправленного в телеконференцию сообщения ;	
3	1 Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. К методам несанкционированного доступа к ресурсам системы рассылки новостей USENET относится: 1. паразитный сетевой трафик; 2. метод заочного воздействия на объекты; 3. использование люков в интерфейсе CGI; 4. использование постоянно поступающей информации.		4
3	2. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Программная закладка (ПЗ) записывается в ПЗУ, в системное или прикладное обеспечение и сохраняет вводимую, выводимую информацию в скрытую область памяти локального или удаленного компьютера. Этот метод воздействия программных закладок на компьютер называется: 1. «Перехват» 2. «Искажение» 3. «Наблюдатель» 4. «Компрометация».		1
3	3. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. К методам несанкционированного доступа к клиентскому программному обеспечению www относится: 1. передача бессмысленных огромных файлов по низкоскоростным каналам; 2. перегрузка серверов сети незавершенными процессами установки соединений; 3. метод несанкционированного доступа, ориентированный на серверы www. 4. использование управляющих сообщений;		3

3	4. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. К методам создания скрытых каналов передачи данных относится: 1. передача программ, создающих скрытый канал обмена сквозь firewall через порт 80. 2. получение привилегированного доступа к потоку новостей; 3. создание специального сервера www; 4. проверка текущих задач пользователя;	1
5	5. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Наиболее распространенной угрозой информационной безопасности корпоративной системы является покупка _____ программного обеспечения.	нелицензионного
5	6. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Секретность закрытого сообщения определяется секретностью ключа – называется принципом _____.	Кирхгофа
5	7. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Используя асинхронную природу ОС компьютерную систему, заставляют работать в сложных условиях, из-за чего работа нарушается. Данная ситуация используется для внесения изменений в ОС, при чем эти изменения не будут заметны. Этот метод называется _____ атака.	асинхронная
5	8. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Программа, заражающая другие программы, путем включения в них своей модифицированной копии, при чем последняя имеет способность к дальнейшему распространению, называется _____.	вирус
1	9. Прочитайте текст и установите соответствие между методами вредоносных воздействий и их реализацией 1. Метод снижения эффективности работы сети на уровне транспортных и коммуникационных протоколов 2. Метод несанкционированного доступа к ресурсам системы рассылки новостей USENET 3. Метод несанкционированного доступа к клиентскому программному обеспечению WWW 4. Метод несанкционированного доступа к электронной почте А) создание скрытых каналов передачи данных Б) несанкционированное использование SMTP-сервера В) использование люков в интерфейсе CGI Г) удаление ранее отправленного в телеконференцию сообщения	1-А, 2-Г, 3-В, 4-Б
1	10 Прочитайте текст и установите соответствие между разновидностями вирусов и их воздействием 1. файловый нерезидентный вирус 2. файловый резидентный вирус 3. бутовый вирус 4. гибридный А. заражает не только исполняемые файлы, находящиеся во внешней памяти, но и оперативную память Б) целиком размещается в исполняемом файле, в связи с чем он активизируется только в случае активизации вирусоносителя, а по выполнении необходимых действий	1-Б, 2-А, 3-Г, 4 –В

		возвращает управление самой программе В) инфицируют как файлы, так бут-сектора Г)инфицируют загрузочный (бут-сектор) магнитного носителя;	
3	11. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. К методам несанкционированного доступа к электронной почте относится: 1. несанкционированное использование SMTP-сервера. 2. получение списка пользователей сервера 3. создание паразитного трафика 4. засорение новостных каналов устаревшей информацией		1
3	12. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. По времени пребывания программных закладок в оперативной памяти можно выделить следующие типы закладок: 1. постоянные; 2. временные; 3. краткосрочные; 4. резидентные.		4
3	13. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Эта программа в процессе своего функционирования выполняет применительно к каждому исполняемому файлу сравнение его текущих характеристик с аналогичными характеристиками, полученными в ходе предшествующего просмотра: 1. детектор; 2. вакцина; 3. монитор; 4. ревизор.		4
4	14. Прочитайте текст, выберите все правильные варианты ответа и запишите аргументы, обосновывающие выбор ответа. Свойство резидентности предполагает выполнение вирусом на этапе загрузки двух действий 1. закрепление в памяти. 2. перехват системных функций. 3. поглашение системных ресурсов 4. подключение к линиям связи		1, 2
5	15. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Гарантия того, что секретные данные будут доступны только авторизованным пользователям, которым этот доступ разрешен называется _____.		конфиденциальность
5	16. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. К методам снижения эффективности работы сети на уровне транспортных и коммуникационных протоколов относится _____ пропускной способности каналов передачи данных.		деградация
5	17. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. _____ независимая сеть передачи данных, лишь организационно входящая в состав internet и использующая нижние уровни протоколов TCP/IP.		usenet
3	18. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа.		2

<table>
<tr><td></td><td>При подключении к серверу рассылки новостей система сообщает об используемой версии сервера, а также о том, разрешен ли режим загрузки внешних сообщений и имя системы, на которой запущен данный сервер. Это принцип действия метода:
1) восстановления структуры сети рассылки новостей
2) идентификационной строки сервера рассылки новостей
3) подмены документов серверов нецензурными изображениями
4)перехвата электронной почты</td><td></td></tr>
<tr><td>1</td><td>19. Прочитайте текст и установите соответствие между методами вредоносных воздействий и их названием
1. Метод, при котором происходит подключение к линиям связи и перехват работы после окончания сеанса законного пользователя:
2. Метод при котором происходит создание условий, когда законный пользователь осуществляет связь с нелегальным терминалом, будучи уверенным, в том, что он работает с необходимым ему абонентом называется:
3. Используя асинхронную природу ОС компьютерную систему, заставляют работать в сложных условиях, из-за чего работа нарушается. Данная ситуация используется для внесения изменений в ОС, при чем эти изменения не будут заметны. Этот метод называется:
А) асинхронная атака
Б) «мистификация»
В) «за хвост»</td><td>1-В, 2-Б, 3-А</td></tr>
<tr><td>1</td><td>20. Прочитайте текст и установите соответствие между разновидностями вредоносных воздействий и реализующими их методами
1. Методы несанкционированного доступа ориентированные на нештатное использование программ- браузеров HTML-страниц WWW, а также на применение программ, расширяющих функциональные возможности браузеров для решения не свойственных им задач- это:
2. К методам снижения эффективности работы сети на уровне транспортных и коммуникационных протоколов относится:
3. К методам несанкционированного доступа к ресурсам системы рассылки новостей USENET относится:
А) вскрытие структуры сети и основных информационных каналов по анализу распространения новостей USENET
Б) Методы доступа, основанные на отдельных элементах протокола NNTP
В) методы несанкционированного доступа к клиентскому программному обеспечению WWW</td><td>1-В, 2-В, 3-А</td></tr>
<tr><td>3</td><td>21. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа.
Какой орган лицензирует деятельность по защите информации?
1. Министерство по сертификации
2. МВД
3. Федеральная служба по техническому и экспортному контролю (ФСТЭК России).
4. Министерство обороны</td><td>3</td></tr>
<tr><td>3</td><td>22. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа.
Антивирусы обеспечивающие выявление вирусов посредством просмотра исполняемых файлов поиска так называемых сигнатур- это:
1. детекторы.
2. фаги;</td><td>1</td></tr>
</table>

	3. вакцины; 4. мониторы;	
3	23. Прочитайте текст, выберите правильный вариант ответа и запишите аргументы, обосновывающие выбор ответа. Резидентная программа, обеспечивающая перехват потенциально опасных прерываний, характерных для вирусов, и запрашивающая у пользователей подтверждение на выполнение операций, следующих за прерыванием - это: 1. прививка; 2. ревизор; 3. вакцина; 4. монитор.	4
4	24. Прочитайте текст, выберите все правильные варианты ответа и запишите аргументы, обосновывающие выбор ответа. По способу инфицирования жертвы вирусы можно разделить на классы 1. вирусы, которые не внедряют свой код непосредственно в программный файл, а изменяют имя файла и создают код старым именем новый, содержащий тело вируса. 2. Вирусы, внедряющиеся непосредственно в файлы жертвы. 3. Вирусы, внедряющиеся в системную среду ОС	1,2
5	25. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Обеспечение субъекту возможности ознакомления с информацией и ее обработки, в частности, копирования, модификации или уничтожения информации называется _____-к информации..	доступ
5	26. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. _____ - это гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.	целостность
2	27. Прочитайте текст и установите последовательность порядка Перечислите последовательность цикла жизни вируса: 1. проявление 2. период репликации 3. инкубационный период 4. внедрение	4,3,2,1
5	28. Внимательно прочитать текст задания и понять суть вопроса. Продумать логику и полноту ответа. Записать ответ, используя четкие компактные формулировки. Макропрограммы и файлы документов современных систем обработки информации. такие вирусы называются __ _____	макровирусами
1	29. Прочитайте текст и установите соответствие между разновидностями ПО защиты от вредоносных воздействий и их категориями 1. Антивирусы обеспечивающие выявление вирусов посредством просмотра исполняемых файлов поиска так называемых сигнатур- это: 2. Резидентная программа, обеспечивающая перехват потенциально опасных прерываний, характерных для вирусов, и запрашивающая у пользователей подтверждение на выполнение операций, следующих за прерыванием - это: 3. Эта программа в процессе своего функционирования выполняет применительно к каждому исполняемому файлу сравнение его текущих характеристик с аналогичными А)монитор Б) детекторы В) фаги Г) ревизор	1-Б, 2-А, 3-Г, 4-В

	характеристиками, полученными в ходе предшествующего просмотра это: 4. Антивирусы выполняющие функции, свойственные детекторам, но кроме того, излечивают инфицированные программы посредством «выкусывания» вирусов из них- это:		
4	30. Прочитайте текст, выберите все правильные варианты ответа и запишите аргументы, обосновывающие выбор ответа. Выберите все ***неверные*** варианты ответов. Закон «Об информации, информатизации и защите информации» выделяет следующие цели: 1. Предотвращение утечки, хищения, утраты, подделки; 2. Предотвращение угроз безопасности личности, угроз государству; 3. Защита конституционных прав гражданина на сохранение личной тайны. 4. Право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.		3, 4

ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ

на фонды оценочных средств по дисциплине
«Технологии защиты информации в компьютерных сетях»
для подготовки магистров по направлению подготовки
09.04.03 «Прикладная информатика»
профиль «Цифровые технологии в АПК»

Представленные на рецензию фонды оценочных средств оформлены с соблюдением всех требований, предъявляемых к оформлению ФОС по стандартам ФГОС ВО.

Дисциплина ***«Технологии защиты информации в компьютерных сетях»*** является частью учебного плана подготовки по программе магистратуры направления ***09.04.03 «Прикладная информатика»*** профиль «Цифровые технологии в АПК».

Оценочные средства для контроля успеваемости студентов представлены в полном объеме. При помощи фонда оценочных средств осуществляется контроль и управление процессом приобретения студентами необходимых знаний, умений, практического опыта и компетенций, определенных ФГОС ВО.

Представленные оценочные средства по дисциплине стимулируют познавательную деятельность за счет заданий разного уровня сложности, компетентностного подхода, формируют навыки само- и взаимопонимания.

Фонды оценочных средств соответствуют обязательному минимуму содержания ФГОС ВО, обеспечивают проведение аттестации студентов учреждений ВО, дают возможность определить соответствие студентов конкретной характеристике.

Представленные ФОС для подготовки по программе магистратуры направления ***09.04.03 «Прикладная информатика»*** профиль «Цифровые технологии в АПК» могут быть использованы в учебном процессе и соответствуют требованиям ФГОС ВО.

Эксперт:
доцент кафедры Вычислительной техники,
ФГАОУ ВО Сибирский федеральный университет,
Институт космических и информационных технологий, канд. техн. наук, доцент

Вениамин Георгиевич Середкин