Министерство науки и высшего образования Российской Федерации
ФГАОУ ВО «Волгоградский государственный университет»
Институт приоритетных технологий
Кафедра информационной безопасности

УТВЕРЖДАЮ
Директор института
_____ И.В. Запороцкова
«26» 10 2023 г.

УТВЕРЖДАЮ
Председатель приемной комиссии
_____ А.Э. Калинина
«27» 10 2023 г.

ПРОГРАММА
вступительного испытания при приеме на обучение по программам бакалавриата и специалитета на базе среднего профессионального образования
"Защита информации в автоматизированных системах программными и программно-аппаратными средствами"

г.Волгоград, 2023 г.

1. Общие сведения

Целью проведения экзамена является определение общего уровня подготовленности абитуриента по защите информации в автоматизированных системах программными и программно-аппаратными средствами.

Поступающий должен знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации; особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

Форма проведения экзамена

Вступительные испытания проводятся письменно, с возможностью применения дистанционных технологий (в форме онлайн-тестирования). При решении расчетных задач разрешается пользоваться микрокалькуляторами.

Продолжительность экзамена

На подготовку ответа отводится два академических часа. Для предоставления поступающим возможности наиболее полно проявить уровень знаний и умений на вступительных экзаменах должна быть обеспечена спокойная и доброжелательная обстановка, во время приемных испытаний абитуриенты должны соблюдать следующие правила поведения:

- занимать в аудитории место, предложенное одним из членов предметной экзаменационной комиссии или сотрудником приемной комиссии;
- работать самостоятельно и соблюдать тишину;
- не использовать средства оперативной (мобильной) связи;
- не оказывать помощь другим абитуриентам в выполнении экзаменационных заданий;
- не покидать аудиторию во время прохождения вступительного испытания:
- использовать для записей только бланки установленного образца.

Структура экзаменационного билета

Билет состоит из двух вопросов.

Первый вопрос из раздела 1, второй вопрос из раздела 2.

2. Содержание программы

Раздел 1. Применение программных и программно-аппаратных средств защиты информации.

1.Предмет и задачи программно-аппаратной защиты информации. Основные понятия программно-аппаратной защиты информации. Классификация методов и средств программно-аппаратной защиты информации.

2. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты).

3.Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

4.Автоматизация процесса обработки информации. Понятие автоматизированной системы.

Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении.

5. Методы создания безопасных систем. Методология проектирования гарантированно защищенных КС. Дискреционные модели. Мандатные модели.

6.Учет, обработка, хранение и передача информации в АИС. Ограничение доступа на вход в систему. Идентификация и аутентификация пользователей. Разграничение доступа.

7.Регистрация событий (аудит). Контроль целостности данных. Уничтожение остаточной информации. Управление политикой безопасности. Шаблоны безопасности

8. Криптографическая защита. Обзор программ шифрования данных. Управление политикой безопасности. Шаблоны безопасности.

9. Источники дестабилизирующего воздействия на объекты защиты. Способы воздействия на информацию. Причины и условия дестабилизирующего воздействия на информацию

10.Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам. Доступ к данным со стороны процесса.

11.Особенности защиты данных от изменения. Шифрование. Организация доступа к файлам

Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД.

12.Работа автономной АС в защищенном режиме. Алгоритм загрузки ОС. Штатные средства замыкания среды. Расширение BIOS как средство замыкания программной среды

13. Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка). Применение закладок, направленных на снижение эффективности средств, замыкающих среду.

14.Изучение и обратное проектирование ПО. Способы изучения ПО: статическое и динамическое изучение

15. Задачи защиты от изучения и способы их решения. Защита от отладки. Защита от дизассемблирования. Защита от трассировки по прерываниям.

16. Вредоносное программное обеспечение как особый вид разрушающих воздействий

Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения

17. Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch. Бот-неты. Принцип функционирования. Методы обнаружения.

18.Классификация антивирусных средств. Сигнатурный и эвристический анализ. Защита от вирусов в "ручном режиме". Основные концепции построения систем антивирусной защиты на предприятии.

19.Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования. Привязка ПО к аппаратному окружению и носителям.

20.Защитные механизмы в современном программном обеспечении на примере MS Office. Защита информации от несанкционированного копирования с использованием специализированных программных средств. Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint).

21.Проблема защиты отчуждаемых компонентов ПЭВМ. Методы защиты информации на отчуждаемых носителях. Шифрование. Средства восстановления остаточной информации. 22.Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов. Безвозвратное удаление данных. Принципы и алгоритмы.

23.Применение средства восстановления остаточной информации на примере Foremost или аналога. Применение специализированного программно средства для восстановления удаленных файлов. Применение программ для безвозвратного удаления данных. Применение программ для шифрования данных на съемных носителях.

24.Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ. Устройства Touch Memory. СОВ и СОА, отличия в функциях. Основные архитектуры СОВ. Использование сетевых снифферов в качестве СОВ. Аппаратный компонент СОВ. Программный компонент СОВ

25.Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений. Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений

26.Сети, работающие по технологии коммутации пакетов. Стек протоколов TCP/IP. Особенности маршрутизации. Штатные средства защиты информации стека протоколов TCP/IP. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.

27. Виртуальная частная сеть. Функции, назначение, принцип построения. Криптографические и некриптографические средства организации VPN. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки.

28.Методы защиты информации при работе в сетях общего доступа. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности

Основные типы firewall. Симметричные и несимметричные firewall. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций. Требования по сертификации межсетевых экранов.

29.Основные типы угроз. Модель нарушителя. Средства идентификации и аутентификации. Управление доступом.Средства контроля целостности информации в базах данных.Средства аудита и контроля безопасности. Критерии защищенности баз данных. Применение криптографических средств защиты информации в базах данных.

30.Изучение механизмов защиты СУБД MS Access. Изучение штатных средств защиты СУБД MSSQL Server.

Раздел 2. Применение криптографических средств защиты информации

1. Предмет и задачи криптографии. История криптографии. Основные термины.

2.Элементы теории множеств. Группы, кольца, поля. Делимость чисел. Признаки делимости. Простые и составные числа. Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.

3.Отношения сравнимости. Свойства сравнений. Модулярная арифметика. Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.

4.Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида. Китайская теорема об остатках. Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.

5.Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда. Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра. Арифметические операции над большими числами.

6.Эллиптические кривые и их приложения в криптографии. Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений. Проверка чисел на простоту.

7.Классификация основных методов криптографической защиты. Методы симметричного шифрования. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр

8.Методы перестановки. Табличная перестановка, маршрутная перестановка. Гаммирование. Гаммирование с конечной и бесконечной гаммами.

9.Применение классических шифров замены. Применение классических шифров перестановки. Применение метода гаммирования.

10.Основные методы криптоанализа. Криптографические атаки. Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса. Перспективные направления криптоанализа, квантовый криптоанализ.

11.Криптоанализ шифра простой замены методом анализа частотности символов. Криптоанализ классических шифров методом полного перебора ключей. Криптоанализ шифра Вижинера.

12.Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.

13.Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII.

14.Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств.

15.Программная реализация классических шифров. Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.

16.Структурная схема симметричных криптографических систем. Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4.

17.Асимметричные системы шифрования. Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом. Элементы теории чисел в криптографии с открытым ключом.

18.Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи. Применение различных функций хеширования, анализ особенностей хешей. Применение криптографических атак на хеш-функции.

19.Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация.

20.Применение протокола Диффи-Хеллмана для обмена ключами шифрования. Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.

21.Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.

22.Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер. Применение криптографических протоколов для обеспечения безопасности электронной коммерции.

23.Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей.

24.Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав. Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ.

25.Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ. Реализация простейших стеганографических алгоритмов

3. Методика и критерии формирования оценки

Максимальная сумма баллов за каждый вопрос — 50. Итого максимальная сумма баллов за испытание составляет 100 баллов. Положительная оценка – 40 и выше баллов.

4. Список рекомендуемой литературы

Основные источники:

1. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2017.- 175 с.

2. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016.- 248 с.

3. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с

Дополнительные источники:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

5. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

6. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

7. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

8. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

9. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

Электронные источники:

1. Научная библиотека ФГАОУ ВО ВолГУ. Электронные библиотеки: ЭБС «Book.ru», ЭБС «ЮРАЙТ», ЭБС «Лань».

2. Справочная правовая система «Консультант Плюс» www.consultant.ru/

3. База данных Polpred.com Обзор СМИ http://www.polpred.com/

4. Национальная электронная библиотека https://нэб.рф/

5. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

6. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

7. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

8. Федеральный портал «Российское образование www.edu.ru

9. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/

10. Российский биометрический портал www.biometrics.ru

11. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

12. Сайт Научной электронной библиотеки www.elibrary.ru

Председатель экзаменационной комиссии О.А. Какорина