

Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования

«Российский экономический университет имени Г. В. Плеханова»

Высшая школа кибертехнологий, математики и статистики (факультет)

Кафедра прикладной информатики и информационной безопасности

Магистратура

Программа комплексного тестирования «Информационная безопасность»
по направлению 10.04.01 «Информационная безопасность»

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Настоящая программа вступительного испытания (ВИ) по «Информационной безопасности» составлена на основе Приказа Министерства науки и высшего образования Российской Федерации от 17.11.2020 № 1427 (ред. 27.02.2023) «Об утверждении федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность».

II. СОДЕРЖАНИЕ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Тема 1. Основные термины и определения

Безопасность информации. Безопасность информационной технологии. Информационная сфера. Информационная инфраструктура. Объект информатизации. Активы организации. Ресурс системы обработки информации. Информационный процесс. Информационная технология. Техническое обеспечение автоматизированной системы. Программное обеспечение автоматизированной системы. Информационное обеспечение автоматизированной системы. Услуга; сервис. Услуги информационных технологий. Критически важная система информационной инфраструктуры. Критический объект. Информационная система персональных данных. Персональные данные. Автоматизированная система в защищенном исполнении.

Информационная безопасность организации. Объект защиты информации. Защищаемый процесс (информационной технологии). Нарушение информационной безопасности организации. Инцидент информационной безопасности. Событие. Риск. Оценка риска. Источник риска информационной безопасности организации. Политика информационной безопасности (организации). Цель информационной безопасности (организации). Система документов по информационной безопасности в организации.

Угроза информационной безопасности организации. Угроза (безопасности информации). Модель угроз (безопасности информации). Уязвимость (информационной системы); брешь. Нарушитель информационной безопасности организации. Несанкционированный доступ. Сетевая атака. Блокирование доступа (к информации). Атака «отказ в обслуживании». Утечка информации. Разглашение информации. Перехват (информации). Информативный сигнал. Недекларированные возможности. Побочные электромагнитные излучения и наводки.

Менеджмент информационной безопасности организации. Менеджмент риска информационной безопасности организации. Система менеджмента информационной безопасности. Роль информационной безопасности в организации. Служба информационной безопасности организации.

Контроль обеспечения информационной безопасности организации. Мониторинг информационной безопасности организации. Аудит информационной безопасности организации. Свидетельства (доказательства) аудита информационной безопасности организации. Оценка соответствия информационной безопасности организации установленным требованиям. Критерий аудита информационной безопасности организации. Аттестация автоматизированной системы в защищенном исполнении. Критерий обеспечения информационной безопасности организации. Эффективность обеспечения информационной безопасности.

Обеспечение информационной безопасности организации. Мера безопасности; мера обеспечения безопасности. Меры обеспечения информационной безопасности. Организационные меры обеспечения информационной безопасности. Техническое средство обеспечения информационной безопасности. Средство обнаружения вторжений, средство обнаружения атак. Средство защиты от несанкционированного доступа.

Тема 2. Методика оценки угроз безопасности информации

Порядок оценки угроз безопасности информации. Определение негативных последствий от реализации (возникновения) угроз безопасности информации. Определение возможных объектов воздействия угроз безопасности информации. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности. Определение источников угроз безопасности информации. Оценка способов реализации (возникновения) угроз безопасности информации. Оценка актуальности угроз безопасности информации.

Тема 3. Безопасность автоматизированных систем

Защита автоматизированных систем как процесс управления рисками. Особенности современных автоматизированных систем как объектов защиты. Определение безопасности автоматизированных систем. Цель защиты автоматизированной системы и циркулирующей в ней информации. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Угрозы безопасности информации, автоматизированных систем и субъектов информационных отношений. Классификация угроз безопасности. Классификация каналов проникновения в автоматизированную систему и утечки информации. Виды мер противодействия угрозам безопасности. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.

Тема 4. Технологии анализа трафика и состояния сети

Аудит. Подотчетность. Задачи аудита. Файерволы. Сегментация сети. Фильтрация трафика. Определение файервола. Типы файерволов. Системы обнаружения вторжений. Типы систем обнаружения вторжений. Функциональная схема IDS. Правила обнаружения атак

Тема 5. Транспортная инфраструктура и ее уязвимости

Протоколы и их уязвимости. Атаки на транспортную инфраструктуру. TCP-атаки. Затопление SYN-пакетами. Подделка TCP-сегмента. Повторение TCP-сегментов. Сброс TCP-соединения. ICMP-атаки. Перенаправление трафика. ICMP Smurf-атака. Ping смерти и ping-затопление. UDP-атаки. UDP-затопление. ICMP/UDP-затопление. UDP/echo/chargen-затопление. IP-атаки. Атака IP-опции. Атака IP-фрагментация. DNS-атаки. Организация DNS. Атаки на DNS. Методы защиты службы DNS. Сетевая разведка.

Тема 6. Фильтрация и мониторинг трафика

Фильтрация трафика и файерволы. Типы фильтрации трафика. Файерволы на основе маршрутизаторов. Файерволы с функцией NAT. Мониторинг сети. Сетевые снифферы. Система мониторинга NetFlow. Типовые архитектуры сетей, защищаемых файерволами. Демилитаризованная зона. Обобщенная архитектура сети с защитой периметра и разделением внутренних зон.

Тема 7. Вредоносные программы.

Условия существования и классификация вредоносных программ. Компьютерные вирусы. Сетевые черви. Троянские программы. Спам. Руткит.

Условия существования вредоносных программ. Классификация вредоносных программ. Причины появления вредных программ. Действия вредоносных программ. Определение компьютерного вируса. Классификация классических компьютерных вирусов. Файловые вирусы. Загрузочные вирусы. Сетевые вирусы. Особенности алгоритма работы вирусов. Деструктивные возможности вирусов. Способы внедрения вирусов. Троянские программы.

Спам. Наиболее распространенные виды спама. Причиняемый вред спамом. Борьба со спамом. Руткит. Классификация вредоносных программ.

Тема 8. Криптографические методы защиты информации

Информация и информационная безопасность. Объекты защиты. Информационные угрозы и нарушители. Методы и средства защиты информации, меры обеспечения информационной безопасности. Способы передачи конфиденциальной информации на расстоянии. Наивная криптография. Формальная криптография. Математическая криптография. Основные требования, предъявляемые к криптосистемам. Классификация криптографических систем. Шифры одинарной перестановки. Шифры множественной перестановки. Регулярные шифры однозначной замены. Полиграммные шифры. Нерегулярные шифры. Омфонические шифры. Полиалфавитные шифры. Генерация случайных последовательностей. Отличие ключа от гаммы. Классическая стеганография. Компьютерная стеганография.

Тема 9. Адресация в стеке протоколов TCP/IP

Основные задачи адресации. Структура стека протоколов TCP/IP. Типы адресов стека TCP/IP. Формат IP-адреса. Классы IP-адресов. Особые IP-адреса. Использование масок при IP-адресации. Порядок назначения IP-адресов. Технология бесклассовой маршрутизации CIDR. Отображение IP-адресов на локальные адреса. Протокол ARP. Протокол Proху-ARP. Доменная служба имен DNS. Сервер, клиент и протокол DNS. Иерархическая организация службы DNS. Итеративная и рекурсивная процедуры разрешения имени. Корневые серверы. Обратная зона. Протокол DHCP. Режимы DHCP. Динамическое назначение адресов.

III. СТРУКТУРА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Вступительное испытание проводится в форме тестирования, в которое входят вопросы по всем или по части тем обозначенных в разделе II.

Тестирование состоит из 29 заданий, на выполнение которых отводится до 135 минут. Задания подразделяются на 3 уровня сложности:

вопросы группы А – представлены 17 заданиями, одно задание оценивается в 2 балла, всего 34 балла;

вопросы группы Б – представлены 6 заданиями, одно задание оценивается в 5 баллов, всего 30 баллов;

вопросы группы В – представлены 6 заданиями, одно задание оценивается в 6 баллов, всего 36 баллов.

Группа А (Базовый уровень, задания 1-17): проверка знания понятийно-категориального аппарата, основных определений, классификаций и принципов, предусмотренных программой вступительных испытаний:

- формат: задания закрытого типа (с выбором одного верного ответа из предложенного списка).
- от поступающего ожидается: знать корректные формулировки, отличать верные утверждения от ложных, воспроизводить изученный материал по памяти, соотносить термины и их значения.

Группа Б (Средний уровень, задания 18-23): оценка способности применять теоретические знания в стандартных учебных ситуациях. Проверка владения типовыми алгоритмами.

- формат: расчетные задачи в 1-2 действия или задания, требующие анализа условия и применения стандартной формул (методик). Один верный ответ в предложенном списке.
- от поступающего ожидается: проанализировать условие задачи, идентифицировать тип ситуации, выбрать корректный алгоритм решения или формулу, провести типовой расчет, правильно интерпретировать и записать полученный результат.

Группа В (Повышенный уровень сложности, задания 24-29): определение сформированности умений и навыков решения комплексных задач.

- формат: комплексные задачи, требующие применения знаний из разных разделов программы, либо задачи, поставленные в нестандартной формулировке, где от абитуриента требуется самостоятельное построение логической цепочки рассуждений, задачи содержащие избыточные данные. Один верный ответ в предложенном списке.
- от поступающего ожидается: определить стратегию решения, выявить скрытые зависимости между данными, построить логически обоснованную цепочку шагов (рассуждений), выполнить сложные вычисления, проанализировать возможность существования нескольких решений или проверить результат на достоверность.

IV. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Безопасность компьютерных сетей. Олифер В.Г., Олифер Н.А. 2017 г. 644 стр.. Тираж 500 экз. Учебное издание. Формат 60x90/16 (145x215 мм). ISBN 978-5-9912-0420-0. ББК 32.973.202. УДК 004.056:004.7
2. Олифер Виктор, Олифер Наталья. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание, доп.и испр. — СПб.: Питер, 2024. — 1008 с.: ил. — (Серия «Учебник для вузов»).

Нормативные и правовые документы:

1. ГОСТ Р 53114—2008 Защита информации. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ. Основные термины и определения
2. Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.) <https://www.garant.ru/products/ipo/prime/doc/400325044/>