Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования «Российский экономический университет

имени Г.В. Плеханова»

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ ДЛЯ ПОСТУПАЮЩИХ НА ПРОГРАММЫ ПОДГОТОВКИ МАГИСТРОВ ПО НАПРАВЛЕНИЮ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Структура вступительного испытания:

Москва 2023

1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 ОБЩИЕ ПОНЯТИЯ

Безопасность информации [данных]. 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.

1.2 ТЕРМИНЫ, ОТНОСЯЩИЕСЯ К ОБЪЕКТУ ЗАЩИТЫ ИНФОРМАЦИИ

Информационная безопасность организации. Объект защиты информации. Защищаемый процесс (информационной технологии). Нарушение информационной безопасности организации. Чрезвычайная ситуация; непредвиденная ситуация. Опасная ситуация. Инцидент информационной безопасности. Событие. Риск. Оценка риска. Оценка риска информационной безопасности (организации). Идентификация риска. Анализ риска. Определение приемлемости уровня риска. Обработка риска информационной безопасности организации. Управление рисками. Источник риска информационной безопасности организации. Политика информационной безопасности (организации). Цель информационной безопасности (организации). Система документов по информационной безопасности в организации.

1.3 ТЕРМИНЫ, ОТНОСЯЩИЕСЯ К УГРОЗАМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

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.

1.4 ТЕРМИНЫ, ОТНОСЯЩИЕСЯ К МЕНЕДЖМЕНТУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

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

1.5 ТЕРМИНЫ, ОТНОСЯЩИЕСЯ К КОНТРОЛЮ И ОЦЕНКЕ 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.

1.6 ТЕРМИНЫ, ОТНОСЯЩИЕСЯ К СРЕДСТВАМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

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.

1.7 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.

1.8 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.

1.9 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.

1.10 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.

1.11 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.

1.12 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.

1.13 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. Омофонические шифры. Полиалфавитные шифры. Генерация случайных последовательностей. Отличие ключа от гаммы. Классическая стеганография. Компьютерная стеганография.

Рекомендуемая литература

1. Бондарев В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие / В. В. Бондарев. — Москва: Издательство МГТУ им. Н. Э. Баумана, 2016. — 250, [2] с. :ил. ISBN 978-5-7038-4414-4
2. 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
3. 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/
4. Анисимов В.В. Криптографические методы защиты информации. https://sites.google.com/site/anisimovkhv/learning/kripto?authuser=0&pli=1
5. ГОСТ Р 53114—2008 Защита информации. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ. Основные термины и определения

2. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

2.1 НОРМАТИВНЫЕ ДОКУМЕНТЫ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Законы Российской Федерации, определяющие необходимость обеспечения защиты информации. Основные нормативные документы ФСТЭК, классифицирующие средства защиты информации. Нормативные документы, в области защиты персональных данных. Нормативные документы, в области защиты государственных информационных систем.

2.2 АРХИТЕКТУРА СИСТЕМЫ ЗАЩИТЫ

Встроенные защитные механизмы современных операционных систем. Недостатки встроенных защитных механизмов современных операционных систем. Распределенная архитектура средств ПАЗИ. Централизованно-распределенная архитектура средств ПАЗИ. Состав защитных механизмов клиентских компонентов средств ПАЗИ

2.3 МЕХАНИЗМ АВТОРИЗАЦИИ

Основные понятия. Авторизация пользователей по паролю. Угрозы преодоления парольной защиты. Способы усиления механизмов парольной защиты. Особенности реализации многофакторной авторизации с применением средств ПАЗИ.

2.4 УПРАВЛЕНИЕ ДОСТУПОМ К РЕСУРСАМ

Дискреционная модель разграничения доступа. Настройка дискреционных прав доступа пользователей к защищаемым объектам. Мандатная модель управления доступом к защищаемым объектам. Угрозы преодоления разграничительной политики доступа. Гарантированное удаление информации.

2.5 АНАЛИЗ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ В ЗАЩИЩАЕМЫХ СИСТЕМАХ

Организация ведения аудита действий пользователей в операционных системах. Организация ведения аудита действий пользователей с помощью средств защиты информации. Поиск информации в журналах СЗИ. Анализ событий инцидентов информационной безопасности.

2.6 МЕХАНИЗМЫ КОНТРОЛЯ ЦЕЛОСТНОСТИ ЗАЩИЩАЕМЫХ ОБЪЕКТОВ

Принципы организации контроля целостности информационной системы. Механизм уровневого контроля списков санкционированных событий. Механизмы контроля целостности файловых объектов и аппаратной конфигурации защищаемых объектов.

Контроль целостности средства защиты. Использование плат аппаратной поддержки. Замкнутая программная среды.

2.7 СРЕДСТВА АНТИВИРУСНОЙ ЗАЩИТЫ

Компьютерные вирусы и вредоносное программное обеспечение. Средства защиты от компьютерных вирусов и вредоносного программного обеспечения. Обзор средств антивирусной защиты. Принципы настройки средств антивирусной зашиты.

2.8 СРЕДСТВА ЗАЩИТЫ ОТ СЕТЕВЫХ АТАК

Способы осуществления сетевых атак. Разновидности сетевых экранов. Принцип действия сетевых экранов. Разновидности систем обнаружения и предупреждения вторжений. Принцип действия систем обнаружения и предупреждения вторжений.

Рекомендуемая литература

Основная литература

1. Программно-аппаратная защита информации: учеб. пособие / Хорев П.Б. – М.: ФОРУМ: ИНФРА-М, 2019. – 352 с. – (Высшее образование) – ISBN 978-5-00091-709-1. Режим доступа: https://znanium.com/read?id=347714;

2. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов ; под. ред. А. В. Душкина. - Москва : Горячая линия-Телеком, 2022. - 248 с. ISBN 978-5-9912-0470-5. Режим доступа: - URL: https://znanium.com/catalog/product/1911635

Дополнительная литература

1. Защита информации: учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - Москва : РИОР : ИНФРА-М, 2021. – 400 с. ISBN 978-5-369-01759-3. Режим доступа: https://znanium.com/catalog/document?id=367588.

2. Программно-аппаратные средства обеспечения информационной безопасности. Практикум : учебное пособие / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов [и др.] ; под. ред. А. В. Душкина. - Москва : Горячая линия-Телеком, 2020. - 412 с. - ISBN 978-5-9912-0797-3. Режим доступа: - URL: https://znanium.com/catalog/product/1911636 (дата обращения: 29.04.2023).

Нормативные правовые документы

1. Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Режим доступа: https://pd.rkn.gov.ru/docs/Postanovlenie_Pravitel6stva_RF_1119.pdf

2. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

[Текст]: приказ ФСТЭК России № 17 от 11.02.2013. Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702

3. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Текст]: приказ ФСТЭК России № 21 от 18.02.2013. Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691

Перечень информационно-справочных систем

1. http://www.consultant.ru - Справочно-правовая система Консультант Плюс;
2. http://www.garant.ru - Справочно-правовая система Гарант.

3. СЕТИ И ТЕЛЕКОММУНИКАЦИИ

3.1 ОСНОВЫ ПОСТРОЕНИЯ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Понятия: вычислительная сеть, телекоммуникации. Назначение компьютерных сетей. Разновидности компьютерных сетей по технологиям передачи, масштабу сети, топологии; их преимущества и недостатки. Понятие коммутации. Выделенные и коммутируемые каналы. Коммутация пакетов в режимах: дейтаграммном, виртуального вызова, установлением виртуального канала и установлением виртуального соединения. Клиент-серверная архитектура; горизонтальное и вертикальное разделение компонент. Трехзвенная архитектура; одноранговые сети.

Эталонная модель ISO/OSI: причины появления, функции уровней. Модель TCP/IP: уровни, протоколы. Адресация IPv4 и IPv6/

Определение канала передачи информации; основные характеристики каналов связи: АЧХ, полоса пропускания, затухание, емкость, пропускная способность, достоверность передачи. Понятие модуляции, основные виды и их принципы.

Основные принципы организации цифровых каналов передачи данных. Методы разделения каналов по времени и частоте.

3.2 КАНАЛЫ И ЛИНИИ СВЯЗИ

Проводные и кабельные линии связи. Виды и категории витых пар. Устройство и виды коаксиальных кабелей. Волоконно-оптические кабели, их виды, устройство, принципы работы; полное внутреннее отражение и мода сигнала. Передача радиосигнала, особенности связи в различных диапазонах. Спутниковые системы связи; классификация спутников по высоте орбиты, различия их характеристик. Преимущества и недостатки спутниковых систем связи. Мобильная связь. Поколения и стандарты мобильной связи, общая архитектурные принципы.

3.3 МЕТОДЫ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ ИНФОРМАЦИИ

Основные методы повышения достоверности передачи информации. Понятие разрешенного и запрещенного множеств, кратности ошибки, кодового и минимального кодового расстояния. Проверка по четности и код Хемминга. Технологии построения современных локальных и корпоративных сетей передачи данных. Информационная безопасность в сетях. Доступ к среде в сетях. Кодировании сигнала с использованием расширяющей последовательности Баркера.

3.4 МЕТОДЫ И АЛГОРИТМЫ МАРШРУТИЗАЦИИ

Задачи маршрутизации. Понятие метрики. Отличия статических и динамических алгоритмов, одноуровневой и иерархической маршрутизации. Дистанционно-векторные алгоритмы и алгоритмы состояния связей. Коллизии.

Понятия распределенной и сетевой операционных систем, их типы; средства промежуточного уровня. Микроядро. Мультикомпьютерные и мультипроцессорные операционные системы.

Основная литература:

1. Олифер В.Г., Олифер Н.А. / Компьютерные сети: принципы, технологии, протоколы. — М. : Питер, 2020 — 1008 с.
2. Олифер В.Г., Олифер Н.А. /Безопасность компьютерных сетей — М. : Горячая Линия - Телеком, 2016 — 644 с.
3. Вычислительные системы, сети и телекоммуникации. Практикум: учебное пособие для студентов 1-2 курсов физико- математического факультета, обучающихся по направлению «Прикладная математика» / В.А. Чулюков, Д.К. Джахуа, Н.М. Володина. – Воронеж: Воронежский государственный педагогический университет, 2012. – 56 с
4. Райфельд, М. А. Системы и сети мобильной связи : учебное пособие / М. А. Райфельд, А. А. Спектор. - Новосибирск : Изд-во НГТУ, 2019. - 96 с. - ISBN 978-5-7782-3833-6.
5. Урбанович, П. П. Компьютерные сети : учебное пособие / П. П. Урбанович, Д. М. Романенко. - Москва ; Вологда : Инфра-Инженерия, 2022. - 460 с. - ISBN 978-5-9729-0962-9.

Фомин, Д. В. Компьютерные сети / Д. В, Фомин. - 2-е изд., стереотипное - Москва : Директ-Медиа, 2019. - 66 с. - ISBN 978-5-4499-0153-8.