АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ

«БЕЛГОРОДСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ, ЭКОНОМИКИ И ПРАВА»

УТВЕРЖДАЮ
Председатель приемной комиссии,
профессор
_____ В.И. Теплов
25 сентября 2020 г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ ПО СПЕЦИАЛЬНОЙ ДИСЦИПЛИНЕ ДЛЯ ПОСТУПАЮЩИХ В БЕЛГОРОДСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ, ЭКОНОМИКИ И ПРАВА В 2021 ГОДУ ПО ПРОГРАММЕ ПОДГОТОВКИ НАУЧНО-ПЕДАГОГИЧЕСКИХ КАДРОВ В АСПИРАНТУРЕ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 10.06.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» НАПРАВЛЕННОСТЬ (ПРОФИЛЬ) «МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Утверждена на заседании
кафедры организации и технологии защиты информации
протокол № 1 от 31 августа 2020 г.

Белгород – 2020

ВВЕДЕНИЕ

Программа предназначена для сдачи специальной дисциплины по направлению подготовки 10.06.01 «Информационная безопасность» направленность (профиль) «Методы и системы защиты информации, информационная безопасность» и разработана на основе федерального государственного образовательного стандарта высшего образования по программам магистратуры.

Программа содержит перечень основных тем, рекомендуемых для подготовки к вступительному испытанию.

Вступительное испытание проводится в форме, установленной Правилами приема на обучение по образовательным программам высшего образования – программам подготовки научно-педагогических кадров в аспирантуре Автономной некоммерческой организации высшего образования «Белгородский университет кооперации, экономики и права» на 2021 год, и в соответствии с утвержденным расписанием.

В ходе вступительного испытания поступающему предлагаются вопросы из разработанного членами экзаменационных комиссий Перечня тестовых заданий, утвержденного председателем приемной комиссии университета.

Количество вопросов вступительного испытания – 10.

Продолжительность проведения вступительного испытания – 20 минут.

Вступительное испытание оценивается по 5-балльной шкале.

Процедура вступительного испытания оформляется протоколом, в котором фиксируются вопросы к поступающему и краткий комментарий ответов на них.

Во время проведения вступительного испытания участникам запрещается иметь при себе и использовать средства связи.

ОСНОВНЫЕ ТЕМЫ ПО СПЕЦИАЛЬНОЙ ДИСЦИПЛИНЕ, РЕКОМЕНДОВАННЫЕ ДЛЯ ПОДГОТОВКИ К ВСТУПИТЕЛЬНОМУ ИСПЫТАНИЮ

ТЕМА 1. Теория и методология обеспечения информационной безопасности и защиты информации

Предмет информации. Понятие важности и ценности информации. Классификация информации по уровню важности. Виды и формы представления информации. Единицы измерения количества информации. Единицы измерения количества информации. Понятие аналогового и цифрового сигналов. Основные процессы, которым подвергается информация в вычислительных системах: ввод, обработка, хранение, вывод. Пути обеспечения информационного единства в АСУ.

Понятие сущности безопасности информации. Основное отличие информации, как объекта права собственности от права собственности

материального объекта. Правомочия собственника с точки зрения права собственности. Понятия права распоряжения, права владения и права пользования. Инфраструктура, предотвращения нарушения прав собственности па информацию. Федеральный закон «Об информации, информационных технологиях и защите информации». Понятие государственной, коммерческой, личной и служебной тайн. Цель обеспечения безопасности информации. Основные направления информационной безопасности. Понятие информационной, экономической, оборонной, социальной и экономической безопасности. Основные причины, создающие возможности применения информационного оружия против России. Понятие информационной безопасности и защиты информации.

Основной перечень мероприятий, используемых в качестве защиты автоматизированных систем обработки данных и их характеристика. Меры по реализации и сопровождению политики безопасности. Архитектура административной группы управления защитой. Мониторинг функционирования АСОД.

Понятие безопасности автоматизированных систем обработки данных. Пути достижения безопасности АСОД. Виды достижения безопасности АСОД и их характеристики. Понятия случайных и преднамеренных воздействий. Ошибки человека. Аварийные ситуации. Классификация угроз по цели, принципу воздействия и характеру воздействия на АСОД, по причине появления ошибки защиты, способу активного воздействия на объект. Наиболее распространенные угрозы безопасности АСОД и их характеристики. Информационная интегральная безопасность и ее структура. Основные этапы выполнения анализа риска. Классификация угроз системе передачи данных.

Нормативные документы оценки безопасности России, США и Европейских стран. Руководящие документы в области компьютерной безопасности России, США («оранжевая книга»). Понятие классов безопасности США. Руководящие документы РФ в области защиты информации. Основные функции разграничения доступа. Типы классов защищенности от несанкционированного доступа к информации (НСД). Особенности европейских критериев, предъявляемых к системе защиты информации.

ТЕМА 2. Объекты защиты информации

Классификация АСОД по способу построения. Понятия сосредоточенных и распределенных систем обработки данных. Многомашинные и многопроцессорные вычислительные комплексы. Структурная схема ЭВМ с точки зрения обработки информации. Вычислительные системы и системы телеобработки данных. Вычислительные сети: глобальные, региональные и локальные; информационные, вычислительные и информационно-вычислительные. Автоматизированные системы управления: глобальные, региональные и локальные.

Понятия проектирования автоматизированных систем обработки

данных. Цель, задачи и содержание технического задания на проектирование АСОД. Стадии проектирования и испытания АСОД. Понятия условий и режимов эксплуатации АСОД.

ТЕМА 3. Методы и средства защиты информации

Основные методы защиты информации: ограничение доступа, контроль доступа к аппаратуре, разграничение доступа, разделение привилегий на доступ, криптографическое преобразование информации, законодательные меры. Комплексные средства автоматизации и организация его обслуживания. Современные методы защиты информации в вычислительных сетях. Понятие установления идентификации подлинности субъекта (объекта). Варианты установления подлинности. Методы идентификации. Блок-схема алгоритма идентификации и установления подлинности пользователя. Особенности автоматизированной передачи документов по каналам связи. Основные задачи и принципы построения защиты информации в трактах передачи данных в АСУ.

Понятие программных средств защиты данных и их особенности. Задачи, решаемые при организации систем защиты данных с использованием только программных средств. Классификация программных защитных средств. Применение экспертных и самообучающихся систем для организации защиты данных.

Понятие электромагнитных излучений и наводок, их опасность, с точки зрения утечки секретной информации, и НСД к ней. Меры безопасности для защиты информации от побочного электромагнитного излучения и наводок. Пути повышения надежности АСОД. Понятие дублирования и утроения, функционального контроля и диагностики систем. Методы функционального контроля: программные методы, программно-логические методы контроля, алгоритмические методы контроля, тестовые методы контроля, комбинированные методы, аппаратные методы, контроль при дублировании оборудования, контроль по модулю. Классификация методом кот роля достоверности информации в АСОД. Понятие структурной, временной и информационной избыточности.

ТЕМА 4. Криптографические методы защиты информации

Назначение, область применения и состав криптологии. Понятия открытого ключа, секретного ключа, шифра, обратимости, преобразования шифра, обратимого преобразования шифра, шифратора и дешифратора, криптографического алгоритма, криптографических протоколов, и их назначение. Виды криптографических протоколов. Стойкость криптосистемы. Классификация криптосистем. Методы асимметричной криптографии.

Понятие и виды' шифропреобразований. Понятие преобразования перестановки и преобразования замены. Компоненты преобразования

перестановки. Понятия ключа и операции перестановки по ключу. Шифр замены Ю. Цезаря. Шифр замены Гронсфельда. Таблица Вижинера. Двойной квадрат Чарльза Уитстона. Криптографический шифр К. Гаусса с рандомизацией и Джилберта Вернамом с побитным шифрованием. Правило Керхофа.

Понятие криптографической системы с секретным ключом. Модели симметричной и блочной симметричной криптографических систем. Модель детерминированной системы шифрования. SP-узлы, SP-сети К. Шеннона. Стандарт США для шифрования данных DES. Отечественный ГОСТ 28147-89 (алгоритм криптографического преобразования). Криптографическая система Вернама. Теоретическая и практическая стойкость криптографических систем по Шеннону. Синхронные и самосинхронизирующиеся поточные криптографические системы. Управление ключами в системах криптографической информации. Односторонние функции и их применение в криптографии. Открытое распределение ключей (схема Диффи-Хеллмана). Односторонняя функция с секретом. Криптографическая система с открытым ключом. Цифровая подпись. Схема цифровой подписи Эль Гамаля. Существующие стандарты цифровой подписи.

ТЕМА 5. Проектирование и теория защиты данных в АСОД

Этапы развития концепции защиты информации. Вычисли тельная система как объект защиты информации. Потенциальны угрозы информации в вычислительных системах. Возможные каналы НСД в вычислительных системах. Алгоритм проектировании разработки систем защиты информации в вычислительных сетях Понятие автоматизированной системы с безопасной обработкой данных. Основные требования, предъявляемые к защите информации в вычислительных сетях. Защита информации в комплекса) средств автоматизации ее обработки.

Понятие модели ожидаемого поведения нарушителя. Характеристики наиболее опасного нарушителя. Модель элементарной защиты. Варианты определения прочности созданной преграды. Понятие автоматизированной преграды и ее назначение. Определение прочности преграды при организационных мерах защиты Определение прочности преграды зашиты при учете отказа системы. Модель многозвенной защиты. Суммарная прочность дублированных преград в многозвенной (многоуровневой) защите.

ТЕМА 6. Системы опознания и разграничения доступа к информации

Назначение системы опознания и разграничения доступа к информации (СОРДИ). Основные функции СОРДИ. Пароли, их назначения, хранение и использование. Алгоритм контроля и управления разграничением доступа к информации. Факторы, влияющие на эффективность работы СОРДИ.

Пароль, его назначение и характеристики. Выбор длины пароля по формуле Андерсона. Комбинированная система паролей. Одноразовые пароли, их достоинства и недостатки.

Обстоятельства раскрытия паролей. Меры предосторожности для защиты паролей. Методы закрытия паролей.

Карты как носители кодов паролей. Основные типы носителей кодов паролей и требования, предъявляемые к ним. Структура карты. Схема взаимного удостоверения. Проверка подлинности карт. Типы карт, используемых в АСОД. Этапы и: меры защиты ПО и информации от НСД при вводе, выводе и транспортировке. Аппаратно-программные технологии защиты данных. Электронные ключи и их особенности и возможности. Понятия смарт-карт-технологий. Метод модульного диалога как средство дополнительной проверки на санкционированность обращения.

ТЕМА 7. Защита информации в ПЭВМ

Отличительные особенности ПЭВМ как объекта защиты. Потенциальные угрозы информации, обрабатываемой в ПЭВМ. Возможные каналы НСД. Системы защиты информации от НСД в ПЭВМ. Основные функции управления и контроля в ПЭВМ при автономном режиме ее эксплуатации. Возможные каналы НСД к информации в ПЭВМ и потенциальные угрозы Средства защиты по возможным каналам НСД ПЭВМ. Программно-аппаратные средства разграничения доступа к информации ПЭВМ. Оценка уровня безопасности информации от НСД в ПЭВМ.

ТЕМА 8. Защита информации в вычислительных сетях

Информация, являющаяся предметом зашиты в сети. Структура системы защиты информации в автоматизированных системах управления (АСУ). Базовая эталонная модель взаимодействия открытых систем. Понятие физических средств соединения (каналы связи) и их классификация. Функции канального уровня. Сетевой уровень и его функции. Транспортный уровень и его функции. Сеансовый уровень и его назначение. Представительный уровень и его основные функции. Прикладной уровень и его функции.

ЛВС как объект зашиты информации. Программное обеспечение сервера и основные модификации соединений ПК в ЛВС.

Потенциальные угрозы безопасности информация: в ЛВС. Система защиты информации от НСД в ЛВС. Распределение средств защиты по возможным к англам НСД ЛВС. Защита информации ЛВС от случайного НСД.

Варианты защиты информации в телекоммуникационных каналах связи (шифрование данных, цифровая подпись, управление доступом к ресурсам сети). Обеспечение целостности данных.

Архитектура клиент-сервер как основа структурирования информационных систем при рассмотрении программно-технических мер безопасности. Экранирующий шлюз и его назначение. Виды регуляторов, используемых при проведении в жизнь, выбранной политики безопасности. Защита в глобальной сети.

ТЕМА 9. Оценка качества и эффективности систем защиты информации

Исходная форма инструментария комплексной оценки качества (КОК) для выбора моделей. Связь комплекса моделей с подсистемами инструментария КОК для оценки различных показателей функционирования информационных систем (ИС). Назначение инструментария КОК. Функциональные возможности КОК. Технологии обеспечения защищенности ИС.

Оценка надежности выполнения функций программно-техническими средствами. Надежность схемы подготовки, передачи, обработки, хранения и отображения информации программно-техническими средствами. Основные данные для проектирования систем защиты информации. Анализ полученных результатов и выводы. Оценка своевременности представления информации. Представление структуры оценки своевременности предоставления информации. Подготовка данных для проведения расчетов. Представление характеристик временных потоков. Анализ результатов. Выводы. Оценка полноты используемой информации. Оценка актуальности используемой информации. Оценка ошибочности используемой информации после контроля. Оценка корректности обработки информации. Оценка ошибочности действий пользователя и обслуживающего персонала. Оценка защищенности от опасных воздействий. Оценка защищенности информационных и программных ресурсов от несанкционированного доступа.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Конституция Российской Федерации.
2. Гражданский кодекс Российской Федерации от 22.12.95 // Собрание законодательства Российской Федерации. 1996. №5. Ст. 410.
3. Уголовный кодекс Российской Федерации от 24.05.96 // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 155.
4. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 09.09.2000 // Российская газета. 2000. 28 сент. С. 4-6.
5. Об оперативно-розыскной деятельности: Закон РФ от 05.07.95 // Собрание законодательства Российской Федерации. 1995. №33. Ст. 3349.
6. О Федеральной фельдъегерской связи: Закон РФ от 16.11.94 // Собрание законодательства Российской Федерации. 1994. №34. Ст. 3547.
7. О Федеральных органах правительственной связи и информации: Закон РФ от 19.02.93 // Ведомости съезда народных депутатов Российской

Федерации и Верховного Совета Российской Федерации. 1993. № 12. Ст. 423.

8. Об органах Федеральной службы безопасности в Российской Федерации: Закон РФ от 22.02.95 // Собрание законодательства Российской Федерации. 1995. № 15. Ст. 1269.

9. О безопасности: Закон РФ от 05.03.92 // Ведомости съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. – 1992. – № 15. – Ст. 769.

10. О внесении изменений и дополнений в Закон Российской Федерации «О государственной тайне»: Закон РФ от 06.10.97 // -1997.-№41.- Ст. 4673.

11. О государственной тайне: Закон РФ от 21.07.93 // Журнал официальной информации. Кадастр. 1993. – № 35. С. 3-41.

12. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"// Собрание законодательства Российской Федерации. –2006. - N 31 (1 ч.). - Ст. 3448,

13. Об образовании в Российской Федерации: Федеральный закон от 29.12.2012 N 273-ФЗ // Собрание законодательства Российской Федерации. – 2012. №53 (ч. 1). - Ст. 7598.

14. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности: Постановление Правительства РФ от 04.09.95 № 870 // Собрание законодательства Российской Федерации. 1995. № 37. Ст. 3619.

15. О перечне сведений, которые не могут составлять коммерческую тайну: Постановление Правительства Российской Федерации от 05.12.91 // Собрание постановлений правительства РСФСР. 1992. №12. Ст. 7.

16. Перечень должностных лиц органов государственной власти, наделенных полномочиями по отнесению к государственной тайне: Распоряжение Президента РФ от 11.02.95 № 73 // Собрание актов Президента и Правительства Российской Федерации. 1994. №7. Ст. 506

17. Положение о Государственной технической комиссии при Президенте Российской Федерации: Указ Президента Российской Федерации от 19.02.99 № 212 // Собрание законодательства Российской Федерации. 1999. № 8. Ст. 1010.

18. Утверждение Положения о Федеральной службе безопасности Российской Федерации: Указ Президента РФ от 23.06.95 № 633 // Собрание законодательства Российской Федерации. 1995. № 26. Ст. 2453.

19. О создании Государственной технической комиссии при Президенте РФ: Указ Президента РФ от 05.01.92 № 97/ Ведомости съезда народных депутатов РСФСР и Верховного Совета РСФСР. 1992. №3. Ст. 109.

20. Об утверждении перечня сведений конфиденциального характера: Указ Президента Российской Федерации от 06.03.97 № 188 // Собрание законодательства Российской Федерации. 1997. №10. Ст. 4775.

21. Об утверждении перечня сведений, отнесенных к государственной тайне: Указ Президента РФ от 24.01.98 № 61 // Собрание законодательства Российской Федерации. 1998. № 5. Ст. 561.

22. ГОСТ Р 50922 – 2005 Защита информации. Основные термины и определения. – М.: Изд. стандартов, 2005.

23. ГОСТ Р 6.30 – 97 Унифицированные системы документации. Система организационно – распорядительной документации. Требования к оформлению документов. – М.: Изд. стандартов, 1997.

24. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 14 февраля 2008 г.

25. Нормативно-методический документ. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). – М.: Гостехкомиссия России, 2002. – 80 с.

26. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ ФСТЭК России от 18.02.2013 № 21.

27. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 01.11.2012 № 1119.

28. Информационное сообщение об утверждении Требований к средствам антивирусной защиты № 240/24/3095. ФСТЭК России, 30 июля 2012 г.

29. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 15 февраля 2008 г.

30. **Бабаш, А. В.** Информационная безопасность. Лабораторный практикум [Текст] : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. – М. : КноРус, 2013. – 136 с.

31. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Информационная безопасность. – М.: МГФ «Знание», ГЭИТИ, 2008. – 512 с.

32. Белов Е. Б. Основы информационной безопасности: Учебн. пособие/ Электронный ресурс http://www.1variant.ru

33. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. – М.: Горячая линия – Телеком. Бизнес – Безопасность - Телекоммуникации. Терминологический словарь. – М.: Радио и связь, 2012.

34. Блинов А.М. Информационная безопасность: Учебное пособие. Ч. 1. – СПб.: Изд-во СПбГУЭФ, 2010. – 96 с.

35. Будников С.А., Паршин Н.В. Информационная безопасность автоматизированных систем: Учебное пособие, издание второе, дополненное -Издательство им."Е.А.Болховитинова, Воронеж, 2011.

36. Бузов Г.А. Защита от утечки информации по техническим каналам: Учебн. пособие / Бузов Г.А., Калинин С.В., Кондратьев А.В.- М.: Горячая линия - Телеком, 2005. - 416 с.

37. Галатенко В.А. Стандарты информационной безопасности: Курс лекций: Учебное пособие для вузов по специальностям в области

информационных технологий/ Ред. В. Б. Бетелин. – 2-е изд. – М.: Интернет-ун-т информ. технологий, 2012. – 264 с.

38. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.

39. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с.

40. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ-ДАНА, 2013. - 239 с.

41. Запечников С.В. Информационная безопасность открытых систем. Часть 1: Учебник для вузов / Запечников С.В., Милославская Н.Г., Толстой А.И.,

42. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.

43. Переход Н.Г. Вероятностные методы в теории информационных систем: Учебно-методическое пособие. – Белгород: Издательство БУКЭП, 2011. – 92 с.

44. Переход Н.Г. Оптимальные методы обработки параметров случайных сигналов в электромагнитных каналах утечки информации: Монография. – Белгород: Кооперативное образование, 2009. – 153 с.

45. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с.

46. Показатели эффективности информационной деятельности органов государственного управления в условиях противодействия утечке информации по техническим каналам / В.И. Костылев, С.В. Пономаренко, Г.И. Рябинин, А.С. Дерябин – // Информация и безопасность. – 2009. – Вып. 4. – С. 18 – 27.

47. Показатель эффективности информационной деятельности органов государственного управления в условиях противодействия утечке информации по техническим каналам / С.В. Скрыль, В.Н.Финько, С.В. Пономаренко, С.Н. Волкова, Г.И. Рябинин // Информация и безопасность. – 2010. – Вып. 1. – С. 19 – 25.

48. Пономаренко В.В., Пономаренко С.А. Защита и обработка конфиденциальных документов: Учеб. пособие. – Белгород: Издательство Белгородского университета потребительской кооперации, 2009. – 271 с.

49. Пономаренко С.А. Организационная защита информации: Учебное пособие: в 2-х частях. – Белгород: Издательство БУКЭП, 2011. – Ч. 1. – 286 с.

50. Пономаренко С.А. Организация и управление службой защиты информации: Учебное пособие. – Белгород: Издательство БУПК, 2010. – 282 с.

51. Прокушев Я.Е. Программно-аппаратная защита информации. Средства антивирусной защиты: Учеб. пособие. – Белгород: Кооперативное образование, 2014. –144 с.

52. Прокушев Я.Е. Криптографическая защита информации: Учеб. пособие. – Белгород: Кооперативное образование, 2012. – 115 с.

53. Стандарты информационной безопасности: Учебное пособие / Галатенко В.А. Под редакцией члена-корреспондента РАН В.Б. Бетелина / М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2004.

54. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416 с.

55. Экономическая оценка уязвимости информационного ресурса организации / С.В. Пономаренко, Я.Е. Прокушев // Вестник Белгородского университета потребительской кооперации – 2009. – №1.