МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГТУ», ВГТУ)

УТВЕРЖДАЮ
И.о. ректора ВГТУ

_____ Д.К. Проскурин

«_30_» _03_ 2022г.

Система менеджмента качества

ПРОГРАММА

ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ
ПРИ ПРИЕМЕ НА ОБУЧЕНИЕ
ПО ПРОГРАММАМ ПОДГОТОВКИ
НАУЧНЫХ И НАУЧНО-ПЕДАГОГИЧЕСКИХ
КАДРОВ В АСПИРАНТУРЕ

2.3 «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ»
(группа научных специальностей)

2.3.6 «МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
(научная специальность)

Воронеж 2022

I. Перечень элементов содержания, проверяемых на вступительном испытании по научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»

1.Основы информационной безопасности

1. Критерии классификации средств защиты данных. Формальные и нефор-мальные средства защиты.
2. Признаки классификации физических средств защиты информации. Определения понятий «угроза», «воздействие», «источник угроз», «уязвимость», «ущерб», «риск», «информационный риск».
3. Основные положения закона «О персональных данных».
4. Методы биометрической идентификации.
5. Угрозы безопасности персональных данных 1-го, 2-го и 3-го типов.
6. Основные руководящие документы Гостехкомиссии России. Дайте их краткую характеристику.
7. 9 классов защищенности автоматизированных систем (АС) от НСД.
8. Система менеджмента информационной безопасности? Перечислить и охарактеризовать основные процессы, входящие в модель PDCA.
9. Перечислить основные нормативно-методические документы ФСТЭКРоссии в области защиты персональных данных. Дать их краткую характеристику
10. Политика информационной безопасности. Перечислить основные ее по-ложения. Параметры классификации угроз информационной безопасности.
11. Что понимается под национальной безопасностью РФ? Что относится к национальным интересам России в информационной сфере? Приведите их клас- сификацию, в соответствии с Доктриной информационной безопасности РФ.
12. Виды угроз информационной безопасности РФ. Что относится к внеш- ним и внутренним источникам угроз информационной безопасности РФ.
13. Основные функции и задачи, решаемые ФСБ России в области обеспечения информационной безопасности.
14. Категории стандартов по защите информации. Отличия добровольных, регулирующих стандартов и регулятивного использования добровольных стандартов.
15. Критерии безопасности компьютерных систем Министерства обороны США «Оранжевая книга». Европейские критерии безопасности информационных технологий. Американские Федеральные критерии безопасности информационных технологий. Семейство стандартов 27000 системы менеджмента информационной безопасности.

2. Аппаратные средства вычислительной техники и телекоммуникационных устройств

2.1. Аппаратные средства вычислительной техники

1. Логические элементы. Триггеры. Типовые узлы комбинационного типа:сумматор, шифратор/дешифратор; мультиплексор/демультиплексор.
2. Типовые узлы накапливающего типа: регистры, счётчики.
3. Структура процессора. Принцип работы ядра процессора. Организация арифметико-логического устройства. Операции над числами с плавающей и фикси-

рованной точкой.
4. Система команд. Форматы команд и способы адресации. Система преры- ваний. Режимы работы ядра процессора. Классификация процессоров в зависимости от типов обрабатываемых инструкций и способа их исполнения. Устройства управления
5. Оперативное запоминающее устройство: динамическая оперативная память. Работа динамической памяти в состоянии покоя, чтения/регенерации, записи.
6. Оперативное запоминающее устройство: статическая динамическая память. Устройство ячейки статической памяти.
7. Внешнее запоминающее устройство. Накопители на жёстких магнитных дисках.
8. Чипсет, контроллеры и интерфейсы ввода-вывода. Шины связи с процес- сором или системной шины. Шины связи с памятью. Шины связи с графическим адаптером. Шины связи с южным мостом.
9. Чипсет, контроллеры и интерфейсы ввода-вывода. Контроллер шины связи с северным мостом. Контроллер шины связи с платами расширения. Контроллер линий связи с периферийными устройствами и другими ЭВМ. Контроллер шины связи с жесткими дисками. Контроллер шины связи с медленными устройствами.
10. Основы программирования на ассемблере. Архитектура x86. Регистры и прерывания. Основные команды ассемблера. Управляющие конструкции.
11. Основы программирования на ассемблере. Особенности программиро- вания оборудования под Widows. Системные вызовы API.
12. Особенности RISC и MIPS архитектуры. Гарвардская архитектура на примере AVR микроконтроллеров.
13. Программируемые логические устройства (CPLD).
14. Оперативно программируемые логические матрицы (FPGA).
15. Сравнение архитектур и средств проектирования цифровых устройств наПЛИС.

2.2. Аппаратные средства телекоммуникационных систем

1. Основы передачи дискретных данных. Линии связи: типы, характеристикии аппаратура.
2. Методы передачи дискретных данных на физическом уровне.
3. Методы передачи данных канального уровня. Методы коммутации каналов и пакетов.
4. Протоколы и стандарты локальных сетей. Протокол LLC уровня управления логическим каналом.
5. Структурированная кабельная система. Концентраторы и сетевые адаптеры. Логическая структуризация сети с помощью мостов и коммутаторов.
6. Устройство маршрутизатора и основная конфигурация: интерфейсы маршрутизатора, установка маршрутизатора. Базовая конфигурация маршрутизатора.
7. Работа в Cisco IOS. Конфигурирование маршрутизации протокола IP.
8. Средства оптической передачи. Параметры среды и устройств.
9. Технология Ethewet. Метод доступа. Сетевые адаптеры, концентраторы, топология соединения.
10. Глобальные сети и технологии. ISDN. Интерфейсы. Пользовательское оборудование.
11. Сети X.25 и Frame Relay. Особенности оборудования.
12. Технология ATM. Интерфейсы и архитектурная модель. Оборудование.
13. Активное сетевое оборудование и сетевые анализаторы.
14. Обобщенная структура реализации приемопередатчиков современныхсистем мобильной радиосвязи.
15. Архитектура систем микропроцессорного управления приемопередатчиками с сигнальным процессором (DSP).

3. Системы и сети передачи информации

1. Составляющие сетей и систем передачи информации.
2. Физическая передача данных по линиям связи. Проблемы связи. Обобщенная задача коммутации.
3. Коммутация каналов. Коммутация пакетов. Сравнение сетей с коммутацией каналов и коммутацией пакетов.
4. Декомпозиция задачи сетевого взаимодействия. Модель OSI. Стандартизация сетей. Информационные и транспортные услуги.
5. Модуляция. Дискретизация аналоговых сигналов. Методы кодирования. Обнаружение и коррекция ошибок.
6. Беспроводная среда передачи. Беспроводные сети и системы передачи информации. Технология широкополосного сигнала

7. Стек протоколов TCP/ IP. Типы адресов стека TCP/IP. Формат IP -адреса. Порядок назначения IP -адресов.
8. Формат IP-пакета. Схема IP-маршрутизации. Маршрутизация с использованием масок.
9. Протоколы транспортного уровня TCP и UDP. Общие свойства и классификация протоколов маршрутизации. Протокол RIP. Протокол OSPF.
10. Маршрутизация в неоднородных сетях. Протокол BGP. Протокол ICMP.
11. Транспортные услуги и технологии глобальных сетей. Базовые понятия.Технология Frame Relay.
12. Базовые принципы и механизмы MPLS. Протокол LDP. Мониторинг со-стояния путей LSP.
13. Схемы удаленного доступа. Коммутируемый аналоговый доступ. Коммутируемый доступ через сеть ISDN.
14. Технология ADSL. Доступ через сети CATV. Беспроводной доступ.
15. Сетевые службы. Электронная почта. Веб-служба. IP -телефония. Прото-кол передачи файлов. Сетевое управление в IP-сетях.

4. Методы и средства обеспечения информационной безопасности

4.1. Криптографические методы защиты информации

1. Открытые сообщения. Частотные характеристики открытых сообщений. Математические модели открытых сообщений и критерии на открытый текст.
2. Основные понятия криптографии. Определение шифра и его математические модели. Ручные и машинные шифры. Ключевая система и основные требования к шифрам. Понятие криптосистемы.
3. Шифры замены. Одноалфавитные и многоалфавитные шифры замены.
4. Шифры гаммирования. Табличное и модульное гаммирование.
5. Совершенные шифры. Стойкость шифра и избыточность языка. Имито-стойкость и ее характеристики. Методы обеспечения имитостойкости.
6. Основные способы реализации криптографических алгоритмов и требования, предъявляемые к ним. Датчики псевдослучайных последовательностей (регистры сдвига, линейный конгруэнтный метод, линейные рекуррентные последовательности, мультиплексорные методы).
7. Периодичность случайных последовательностей. Распределение элементов в псевдослучайных последовательностях. Основные узлы и блоки криптосистем.
8. Методы анализа криптографических алгоритмов. Алгоритмические, аналитические и статистические методы анализа поточных шифров. Системы шифрования с открытым ключом. Понятие односторонней функции. Криптосистемы RSA и Эль-Памаля.

9. Асимметричные системы шифрования и их преимущества. Хэш-функции и их использование в криптографии.
10. Понятие криптографического протокола. Связь стойкости протокола со стойкостью базовой криптографической системы.
11. Классификация криптографических протоколов. Цифровая подпись. Стандарты цифровой подписи Протоколы аутентификации и их связь с цифровой подписью.
12. Особенности реализации криптосистем на базе вычислительной техники. Криптографические интерфейсы.
13. Компьютерная стеганография - метод, дополняющий традиционные криптографические методы.
14. “Полное” скрытие данных. Типы файл-контейнеров (графические, звуковые). Алгоритмы “упаковки” данных (регулярные, псевдослучайные, комбини- рованные).

4.2. Техническая защита информации

1. Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической за- щиты информации.
2. Структура, классификация и основные характеристики технических кана- лов утечки информации.
3. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях.
4. Распространение оптических сигналов в атмосфере и в светопроводах.
5.Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи.
6.Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации.
7. Виды, источники и носители защищаемой информации. Демаскирующиепризнаки объектов наблюдения, сигналов и веществ.
8. Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности инженерно-технической защиты информации.
9. Требования по защите информации от утечки по техническим каналам.
Виды технического контроля.
10. Способы оценки эффективности охраны объектов защиты. Оценка эффективности защиты видовых признаков объектов наблюдения.
11. Основные задачи, структура и характеристика государственной системы противодействия технической защите. Основные руководящие, нормативные и методические документы по защите информации и противодействия

технической разведке.
12. Физические основы защиты информации от технических разведок. Классификация средств технических разведок по виду носителя. Типовые задачи технических разведок.
13. Методы инженерно-технической защиты информации. Инженерная защита и техническая охрана объектов. Пространственное, энергетическое и структурное скрытие информации и ее носителей.
14. Математическая модель канала утечки информации применительно к техническим разведкам.
15. Классификация методов инженерной защиты и технической охраны объектов защиты. Модели злоумышленника. Типовой комплекс технических средств охраны предприятия.

5. Методы анализа и управления рисками информационной безопасности

5.1. Математическое обеспечение риск-анализа

1. Концепции управления рисками OCTAVE, CRAMM, MITRE. Инструментарий управления информационными рисками.
2. Методы анализа рисков на основе экспертных оценок.
3. Методы анализа рисков на основе аппарата теории нечетких множеств.
4. Меры риска и защищенности систем на основе вероятностных параметров и характеристик ущерба.
5. Функции чувствительности и динамическое моделирование рисков.
6. Оценка рисков сложных систем на основе параметров рисков их компонентов.
7. Аналитическая оценка рисков при нормальном и логнормальном распределениях плотности вероятности наступления ущерба (ПВНУ).
8. Аналитическая оценка рисков при гамма и бета-распределениях ПВНУ.
9. Аналитическая оценка рисков при экспоненциальном, Вейбулла и Эрлан-га распределениях ПВНУ.
10. Аналитические риск-модели при биномиальном, Паскаля и мультинормальном распределениях вероятности наступления ущерба (ВНУ).
11. Аналитические риск-модели при геометрическом и гипергеометрическом распределениях ВНУ.
12. Аналитические риск-модели при пуассоновском распределении ВНУ. Нерегулярные распределения ущерба и динамика рисков.
13. Синтез систем с заданным риском.
14. Прогнозирование эффективности систем на основе анализа рисковущербности и шансов полезности.

5.2. Математическое обеспечение управления рисками

1. Система менеджмента информационной безопасности (СМИБ). Процесс

ный подход в СМИБ (модель PDCA).
2. Задачи менеджмента риска информационной безопасности. Основные эта-пы менеджмента риска информационной безопасности.
3. Методы экспертных оценок при принятии решений. Коэффициент ранговой корреляции Спирмена.
4. Коэффициент конкордации Кэндалла. Энтропийный коэффициент конкордации.
5. Обработка экспертной информации на основе метода парных сравнений.
6. Постановка многокритериальных задач принятия решений. Характеристики приоритета критериев. Нормализация критериев.
7. Принципы оптимальности в задачах принятия решений.
8. Постановка задач оптимизации на основе комбинирования принципов оптимальности. Теория полезности.
9. Аксиоматические методы многокритериальной оценки. Метод аналитической иерархии.
10. Методы порогов несравнимости ЭЛЕКТРА.
11. Статистическая модель однокритериального принятия решений в условиях неопределенности. Критерий Байеса-Лапласа, критерий минимума среднего квадратического отклонения функции полезности или функции потерь.
12. Критерий максимизации вероятности распределения функции полезности, модальный критерий, критерий минимума энтропии математического ожидания функции полезности, критерий Гермейера).
13. Построение критериев оценки и выбора решений при активном противо-действии среды (максиминный критерий Вальда, критерии минимаксного риска Сэвид›ка).
14. Построение критериев оценки и выбора решений при наличии приблизи- тельной априорной информации о состояниях среды (критерий Гурвица, критерий Ходжа-Лемана).
15. Задача линейного программирования с булевыми переменными. Метод ветвей и границ.

II. Требования к уровню подготовки поступающего

Поступающий должен знать/понимать:

-место и роль информационной безопасности в системе национальной без-опасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России;
-сущность и понятие информации, информационной безопасности и характе-ристику ее составляющих;
-основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
-принципы работы элементов и функционалъных узлов электронной аппара-туры;
-типовые схемотехнические решения основных узлов и блоков электронной аппаратуры;
-общие принципы построения вычислительных сетей, их эволюцию,

современные тенденции и основные программно-аппаратные компоненты сети;
-общие принципы проектирования современных систем и сетей телекоммуникаций, включая мультисервисные сети связи;
-основные виды симметричных и асимметричных криптографических алгоритмов;
-математические модели шифров и криптографические стандарты;
-способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;
-организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;
-основные стандарты и методы анализа рисков;
-математические методы принятия решений при управлении рисками информационной безопасности;

Поступающий должен уметь:
-классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
-классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
-работать с современной элементной базой электронной аппаратуры;
-использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации;
-проводить анализ показателей качества сетей и систем связи;
-читать структурные и функциональные схемы систем и сетей связи;
-использовать свойства криптографических средств при анализе комплексных систем защиты информации;
-практически решать задачи защиты программ и данных криптографическими средствами;
-применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы;
-пользоваться нормативными документами по противодействию технической разведке;
-пользоваться методами количественного риск-анализа процессов обработки, поиска и передачи информации;
-применять математические методы принятия решений при управлении рисками информационной безопасности

III. Примерный вариант задания

Поступающий получает 5 (пять) вопросов, на которые он должен максимально расширенно письменно ответить. Вопросы выбираются из каждого блока.

Вопрос № 1. Критерии классификации средств защиты данных. Формальные и неформальные средства защиты.

Вопрос № 2. Структурированная кабельная система. Концентраторы и сетевые адаптеры. Логическая структуризация сети с помощью мостов и коммутаторов.

Вопрос № 3. Стек протоколов TCP/IP. Типы адресов стека TCP/IP. Формат IP -адреса. Порядок назначения IP -адресов.

Вопрос № 4. Совершенные шифры. Стойкость шифра и избыточность языка. Имитостойкость и ее характеристики. Методы обеспечения имитостойкости.

Вопрос № 5. Построение критериев оценки и выбора решений при активном противодействии среды (максиминный критерий Вальда, критерии минимаксного риска Сэвиджа).

Критерии оценивания работ поступающих

Оценивание ответов на каждый вопрос осуществляется по 5-балльной шкале в зависимости от правильности и развернутости (углубленности) ответа (согласно таблице 1). После ответов на все вопросы определяется среднее арифметическое, округленное в большую или меньшую сторону по правилам математики.

Таблица 1

Оценка	Критерий оценки
Отлично	Претендент демонстрирует полное понимание вопроса. На вопрос претендентом представлен развернутый (углубленный) ответ из нескольких литературных источников.
Хорошо	Претендент демонстрирует полное понимание вопроса. На вопрос претендентом представлен недостаточно развернутый (углубленный) ответ.
Удовлетворительно	Претендент демонстрирует частичное понимание вопроса. Претендентом представлен ответ только на часть вопроса.
Неудовлетворительно	Претендент демонстрирует непонимание вопроса. У претендента нет ответа на вопрос.

IV. Рекомендуемая литература

Основная литература

1. Бройдо, В.Л. Вычислительные системы, сети и телекоммуникации[Текст]: Учебник / В. Л. Бройдо. - 2-е изд. - СПб.: Питер, 2005. -703 с.
2. Попов Е.А. Компьютерные сети [Электронный ресурс] : Учеб. пособие /Е. А. Попов, В. Н. Деревянко. - Электрон. текстовые, граф. дан. (2,97 Мб). - Воронеж:ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл.
3. Радько Н.М. Основы криптографической защиты информации [Электронный ресурс]: Учеб. пособие / Н. М. Радько, А. Н. Мокроусов. - Электрон. текстовые, граф. дан. (1,04 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл.
4. Остапенко А.Г. Математические основы риск-анализа [Электронный ресурс]: Учеб. пособие / А. Г. Остапенко, М. В. Бурса. - Электрон. текстовые, граф. дан. (446 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл.
5. Остапенко А. Г. Математические основы управления рисками нарушения информационной безопасности: учеб. пособие [Электронный ресурс]. Электрон. текстовые, граф. данные (4,12 Мб) / А. Г. Остапенко, О. Н. Чопоров. Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2014.
6. Основы информационной безопасности [Электронный ресурс] / О. Н. Чопоров, А. Г. Остапенко. - Электрон. текстовые, граф. дан. (0,99 Мб). - Воронеж ФГБОУ ВПО "Воронежский государственный технический университет", 2015. -1 файл.
7. Титов А.А. Технические средства защиты информации: Учеб. пособие / А.А. Титов. — Томск: ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2010. — 194 с.
8. Олифер В.Г. Компьютерные сети : Принципы, технологии, протоколы: Учебник для вузов / В. Г. Олифер, Н. А. Олифер - 2-е изд. - СПб. : Питер, 2003. -864с.

Дополнительная литература

1. Основы криптографии: Учеб. пособие / А. П. Алферов и др. - М.: Гелиос АРВ, 2002. - 480с.
2. Основы информационной безопасности: Учебник / В.А. Минаев, С.В. Скрыль, А.П. Фисун, С.В. Дворянкин. - Воронеж: Воронежский институт МВД России, 2001. - 464с.- 120.00.
3. Технические, организационные и кадровые аспекты управления информационной безопасностью : Учеб пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - М. : Горячая линия -Телеком, 2014. - 214 с.
4. Управление рисками информационной безопасности: Учеб. пособие/ Н.

Г. Милославская, Н. Ю. Сенаторов. - 2-е изд., испр. - М. ‘ Горячая линия - Телеком, 2014. - 130 с.
5. Управление инцидентами информационной безопасности и непрерывностью бизнеса : Учеб. пособие / Н. Г. Милославская, М. Ю. Сенаторов. - М. : Горя- чая линия -Телеком, 2014. — 170
6.Основы управления информационной безопасностью / А.П. Курило , Учеб. пособие. - 2-е изд., испр. - М. : Горячая линия -Телеком, 2014. - 244 с.
7. Разработка системы технической защиты информации: Учеб. пособие / В.И. Аверченков. — Москва: ФЛИНТА, 2011, 187 с.
8. Анализ и управление рисками беспроводных сетей [Электронный ресурс] Учеб. пособие / В. Б. Щербаков, С. А. Ермаков, В. И. Бочаров ; под ред. Г. С.
Остапенко. - Электрон. текстовые, граф. дан. (3052032 байт). - Воронеж ГОУВПО "Воронежский государственный технический университет", 2008. - 1файл.
9. Аппаратные средства вычислительной техники [Электронный ресурс] учеб. пособие / В. П. Дуров. - Электрон. текстовые дан. (11441664 Байт). - Воро- неж : ВГТУ, 2005. - 1 файл. - Имеется вариант на бумажном носителе.
10. Построение сетей и систем передачи информации [Электронный ресурс]Учеб. пособие / И. В. Гончаров. - Электрон. текстовые, граф. дан. (4,28 Мб). - Воронеж ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.
11. Технические средства и методы защиты информации: Учеб. пособие/ А.П. Зайцев. — Москва: Горячая линия-Телеком, 2012. — 616 с.

Ресурсы информационно-телекоммуникационной сети «Интернет»:

1. https://www.consultant.ru/ справочная правовая система «КонсультантПлюс».
2. https://www.garant.ru/ — справочная правовая система «Гарант».
3. https://znanium.ru/ — крупнейшая бесплатная электронная библиотека рос-сийского Интернета.
4. http://elibrary.ru/defaultx.asp — «eLibrary.ru». Российская электронная библиотека.
5. https://www.rsl.ru/ — российская государственная библиотека.
6. https://book.ru/—электронно-библиотечная система
7. https://www.scholar.ru/ — российская электронная база научных публикаций
8. http://kremlin.ru/ — официальный сайт Президента Российской Федерации.
9. http://government.ru/ — официальный сайт Правительства Российской Федерации.
10. http://gov.ru —сервер органов государственной власти Российской Федерации
11. https://infosecportal.ru/ - информационно-аналитический ресурс для экспертов по информационной безопасности