Министерство науки и высшего образования российской федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И. о. зав. кафедрой ИСЭиА
_____ Колдаев А.И.
«15» 03 2021 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине:
«Информационная безопасность»

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Направление подготовки 09.03.02 Информационные системы и технологии
Профиль Информационные системы и технологии в бизнесе
Квалификация выпускника бакалавр
Форма обучения заочная
Год начала обучения 2021
Изучается на 4 курсе летняя сессия

Предисловие

1. Назначение: для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине «Информационная безопасность» для студентов направления подготовки 09.03.02 Информационные системы и технологии.

2. Фонд оценочных средств текущего контроля успеваемости и промежуточной аттестации на основе рабочей программы дисциплины «Информационная безопасность» в соответствии с образовательной программой по направлению подготовки 09.03.02 Информационные системы и технологии, утвержденной на заседании Учёного совета НТИ (филиал) СКФУ.

3. Разработчик: Кочеров Ю. Н. канд., техн., наук, доцент базовой кафедры регионального индустриального парка

4. ФОС рассмотрен и утвержден на заседании базовой кафедры регионального индустриального парка.

5. ФОС согласован с выпускающей кафедрой информационных систем, электропривода и автоматики.

6. Проведена экспертиза ФОС. Члены экспертной группы, проводившие внутреннюю экспертизу:

Председатель: Кузьменко В.В., и.о. директора НТИ (филиал) СКФУ, профессор кафедры гуманитарных и математических дисциплин
Члены экспертной группы:

Должикова М.В. – заместитель директора по учебно-воспитательной работе НТИ (филиал) СКФУ;

Колдаев А.И. – доцент кафедры информационных систем, электропривода и автоматики.

Эксперт, проводивший внешнюю экспертизу:

Остапенко Н.А., – кандидат технических наук, ведущий инженер-конструктор КБ модернизации ООО КИЭП «Энергомера» филиал АО «Электротехнические заводы «Энергомера»

7. Экспертное заключение: фонд оценочных средств отвечают основным требованиям федерального государственного образовательного стандарта и способствует формированию требуемых компетенций.

Срок действия ФОС: на срок реализации образовательной программы.

Паспорт фонда оценочных средств
для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине:
«Информационная безопасность»

Направление подготовки 09.03.02 Информационные системы и технологии
Профиль Информационные системы и технологии в бизнесе
Квалификация выпускника бакалавр
Форма обучения заочная
Год начала обучения 2021
Изучается на 4 курсе летняя сессия

Код оцениваемой компетенции	Этап формирования компетенции (№ темы)	Средства и технологии оценки	Вид контроля, аттестация	Тип контроля	Наименование оценочного средства
ОПК-3	Тема №1-3	Собеседование	Устный	Текущий	Вопросы для собеседования

Составитель Кочеров Ю.Н.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Вопросы для собеседования
по дисциплине Информационная безопасность
Пороговый уровень

Тема 1. Средства защиты информации

1. Что такое LFSR?
2. Как построить псевдослучайный генератор на основе регистра сдвига?
3. На чем базируется стойкость генераторов псевдослучайных чисел, исследованных в лабораторной работе?
4. Как реализовать возведение в степень чисел большой разрядности по большому модулю?
5. Какая информация является конфиденциальной?
6. Что относится к защищаемой информации?
7. Что понимается под политикой безопасности?
8. Что понимается под несанкционированным воздействием на защищаемую информацию?
9. Дайте понятие конфиденциальности, целостности и доступности информации.

Тема 2. Функциональная безопасность корпоративных систем

1. Что такое симметричное шифрование?
2. В чем особенность блочных шифров?
3. В чем особенность асимметричных систем шифрования?
4. На чем базируется криптостойкость RSA?
5. Как увеличить производительность системы шифрования RSA?
6. Составляющие функциональной безопасности
7. Этапы построения систем безопасности

Тема 3. Криптографические средства защиты

1. Назначение цифровой подписи.
2. В чем отличие криптосхемы ЭльГамаля от RSA?
3. Почему шифр RSA называется асимметричным?4
4. На чем основана стойкость шифра RSA?
5. Что такое цифровой конверт?
6. Опишите общую схему ЭЦП.
7. Каково назначение хеш-функции?
8. Какими свойствами противодействия должна обладать криптографическая хеш-функция?
9. Что такое MAC и как он формируется?

Повышенный уровень

Тема 1. Средства защиты информации

1. Какие тесты на случайность вам известны?
2. Сравните результаты тестов генераторов из первой лабораторной работы с тестами второй работы
3. Дайте определение информационной безопасности.
4. Какие цели и задачи включает в себя концепция национальной безопасности РФ?
5. Перечислите основные виды угроз информационной безопасности РФ.
6. Дайте определение комплексного обеспечения информационной безопасности.
7. Перечислите основные элементы организационной основы государственной системы обеспечения информационной безопасности РФ

Тема 2. Функциональная безопасность корпоративных систем

1. Какова длина ключа блочного шифра?
2. На чем базируется криптостойкость блочного шифра?
3. Какие элементарные операции используются в симметричном шифровании?
4. Какие атаки на систему RSA вам известны?
5. Как противодействовать атакам на систему RSA?
6. Анализ рисков и показатели функциональной безопасности

Тема 3. Криптографические средства защиты

1. На чем базируется криптостойкость системы ЭльГамаля?
2. Почему шифр RSA называется асимметричным?5
3. На чем основана стойкость шифра RSA?
4. Что такое цифровой конверт?
5. Опишите общую схему ЭЦП.
6. Каково назначение хеш-функции?
7. Какими свойствами противодействия должна обладать криптографическая хеш-функция?
8. Что такое MAC и как он формируется?
9. Каковы функции удостоверяющего центра ЭП? Какие сведения заносятся в сертификат открытого ключа ЭП?
10. Для каких целей используется СКЗИ «Верба-OW»?
11. Какие отечественные криптоалгоритмы реализуются в «КриптоПро CSP»?
12. Каково назначение ПАК «КриптоПро УЦ»?

Компетентностно-ориентированные задания

1. Проанализировать, 4-битовый LFSR с отводом от первого и четвертого битов со значением 1010
2. Для сообщения длинно 4 бита, шифруемого алгоритмом RSA задаются начальные параметры: генерируется два секретных больших простых числа p и q, необходимо вычислить n и $\varphi(n)$
3. Изобразите схему конструкции Фейстеля и поясните ее
4. Изобразите схема DES-преобразования
5. Рассчитайте значение $1570^{1019} \bmod 3337$

6. Для генерации пары ключей для сообщения длинной 4 вычислите открытый и закрытый ключи

Составитель Кочеров Ю.Н.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Паспорт фонда тестовых заданий по дисциплине Информационная безопасность

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

№ п/п	Тест	Ключ
1.	Какова цель использования генераторов псевдослучайных чисел при поточном шифровании? – формирование открытых ключей – защита информации от всех случайных или преднамеренных изменений – получение «бесконечной» гаммы (ключевой последовательности), располагая относительно малой длиной самого секретного ключа – защита информации от случайных помех при передаче и хранении – сжатие информации	получение «бесконечной» гаммы (ключевой последовательности), располагая относительно малой длиной самого секретного ключа
2.	Чем определяется разрядность сдвигового регистра с обратной связью? – скоростью работы регистра – температурой окружающей среды – количеством входов в устройстве генерации функции обратной связи – количеством бит, которое может одновременно храниться в регистре сдвига	количеством бит, которое может одновременно храниться в регистре сдвига
3.	Математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, называется в криптографии – функцией Диффи-Хеллмана – односторонней функцией – функцией Эйлера – криптографической функцией	односторонней функцией
4.	Алгоритм ГОСТ 28147-89 является – алгоритмом вычисления функции хеширования – блочным алгоритмом асимметричного	блочным алгоритмом симметричного шифрования

	шифрования – блочным алгоритмом симметричного шифрования – алгоритмом формирования электронной цифровой подписи	
5.	Что является особенностью использования режима CBC блочного шифра? – одинаковые сообщения при использовании разных векторов инициализации преобразуются в одинаковый шифротекст – сообщение, зашифрованное в данном режиме, можно расшифровать, выбирая блоки шифротекста в произвольном порядке – одинаковые блоки исходного текста преобразуются в одинаковый шифротекст – этот режим работает очень медленно, что практически не позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщений – сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока	сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока
6.	Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0B5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид	10000010
7.	Может ли шифр с конечным ключом быть совершенным? – да, если это алгоритм шифрования с открытым ключом – в зависимости от параметров шифра – нет – да	нет
8.	Что общего имеют все методы шифрования с закрытым ключом? – в них для шифрования информации используется один ключ, а для расшифрования – другой ключ – в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов – в них для операций шифрования и расшифрования используется два разных ключа – открытый и закрытый – в них для шифрования и расшифрования информации используется один и тот же ключ	в них для шифрования и расшифрования информации используется один и тот же ключ
9.	Для чего предназначен алгоритм Блюм-Блюма-Шуба (BBS)? – генерации псевдослучайных чисел	генерации псевдослучайных чисел

	– для сжатия информации – для формирования открытых ключей – для формирования хеш-кода	
10.	Выберите вариант ответа, содержащий только простые числа – 2, 5, 19, 37, 59, 101 – 2, 7, 17, 37, 57, 107 – 2, 5, 19, 37, 59, 133 – 3, 7, 19, 39, 59, 10	2, 5, 19, 37, 59, 101
11.	К правовым методам, обеспечивающим информационную безопасность, относятся: – Разработка аппаратных средств обеспечения правовых данных – Разработка и установка во всех компьютерных правовых сетях журналов учета действий – Разработка и конкретизация правовых нормативных актов обеспечения безопасности	Разработка и конкретизация правовых нормативных актов обеспечения безопасности
12.	Основными источниками угроз информационной безопасности являются все указанное в списке: – Хищение жестких дисков, подключение к сети, инсайдерство – Перехват данных, хищение данных, изменение архитектуры системы – Хищение данных, подкуп системных администраторов, нарушение регламента работы	Перехват данных, хищение данных, изменение архитектуры системы
13.	**Виды информационной безопасности:** – Персональная, корпоративная, государственная – Клиентская, серверная, сетевая – Локальная, глобальная, смешанная	Персональная, корпоративная, государственная
14.	Цели информационной безопасности – своевременное обнаружение, предупреждение: – несанкционированного доступа, воздействия в сети – инсайдерства в организации – чрезвычайных ситуаций	
15.	Основные объекты информационной безопасности: – Компьютерные сети, базы данных – Информационные системы, психологическое состояние пользователей – Бизнес-ориентированные, коммерческие системы	Компьютерные сети, базы данных
16.	Основными рисками информационной безопасности являются: – Искажение, уменьшение объема, перекодировка информации – Техническое вмешательство, выведение из строя оборудования сети – Потеря, искажение, утечка информации	Потеря, искажение, утечка информации
17.	К основным принципам обеспечения информационной безопасности относится:	Экономической эффективности системы

	– Экономической эффективности системы безопасности – - Многоплатформенной реализации системы – - Усиления защищенности всех звеньев системы	безопасности
18.	Основными субъектами информационной безопасности являются: – руководители, менеджеры, администраторы компаний – органы права, государства, бизнеса – сетевые базы данных, фаерволлы	органы права, государства, бизнеса
19.	К основным функциям системы безопасности можно отнести все перечисленное: – Установление регламента, аудит системы, выявление рисков – Установка новых офисных приложений, смена хостинг-компании – Внедрение аутентификации, проверки контактных данных пользователей	Установление регламента, аудит системы, выявление рисков
20.	Принципом информационной безопасности является принцип недопущения: – Неоправданных ограничений при работе в сети (системе) – Рисков безопасности сети, системы – Презумпции секретности	Неоправданных ограничений при работе в сети (системе)
21.	Принципом политики информационной безопасности является принцип: – Невозможности миновать защитные средства сети (системы) – Усиления основного звена сети, системы – Полного блокирования доступа при риск-ситуациях	Невозможности миновать защитные средства сети (системы)
22.	Принцип Кирхгофа: – Секретность ключа определена секретностью открытого сообщения – Секретность информации определена скоростью передачи данных – Секретность закрытого сообщения определяется секретностью ключа	Секретность закрытого сообщения определяется секретностью ключа
23.	ЭЦП – это: – Электронно-цифровой преобразователь – Электронно-цифровая подпись – Электронно-цифровой процессор	Электронно-цифровая подпись
24.	Наиболее распространены угрозы информационной безопасности корпоративной системы: – Покупка нелицензионного ПО – Ошибки эксплуатации и неумышленного изменения режима работы системы – Сознательного внедрения сетевых вирусов	Ошибки эксплуатации и неумышленного изменения режима работы системы
25.	Наиболее распространены средства воздействия на сеть офиса:	Вирусы в сети, логические мины

	– Слабый трафик, информационный обман, вирусы в интернет – Вирусы в сети, логические мины (закладки), информационный перехват – Компьютерные сбои, изменение администрирования, топологии	(закладки), информационный перехват
26.	Утечкой информации в системе называется ситуация, характеризуемая: – Потерей данных в системе – Изменением формы информации – Изменением содержания информации	Потерей данных в системе
27.	Угроза информационной системе (компьютерной сети) – это: – Вероятное событие – Детерминированное (всегда определенное) событие – Событие, происходящее периодически	Вероятное событие
28.	Информация, которую следует защищать (по нормативам, правилам сети, системы) называется: – Регламентированной – Правовой – Защищаемой	
29.	Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке: – Программные, технические, организационные, технологические – Серверные, клиентские, спутниковые, наземные – Личные, корпоративные, социальные, национальные	Программные, технические, организационные, технологические
30.	Что такое «минимальное кодовое расстояние»? – характеристика помехоустойчивого кода, показывающая, насколько увеличена длина кодового слова по сравнению с обычным непомехоустойчивым кодом – число разрядов двух кодовых слов, в которых они различны – число контрольных разрядов в кодовом слове – наименьшее из всех расстояний по Хэммингу для любых пар различных кодовых слов, образующих код	наименьшее из всех расстояний по Хэммингу для любых пар различных кодовых слов, образующих код

Составитель Кочеров Ю.Н.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

КРИТЕРИИ И ШКАЛЫ ОЦЕНИВАНИЯ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

«5» (отлично): студент демонстрирует системные теоретические знания, владеет терминологией, делает аргументированные выводы и обобщения, приводит примеры, показывает свободное владение монологической речью и способность быстро реагировать на уточняющие вопросы.

«4» (хорошо): студент демонстрирует прочные теоретические знания, владеет терминологией, делает аргументированные выводы и обобщения, приводит примеры, показывает свободное владение монологической речью, но при этом делает несущественные ошибки, которые быстро исправляет самостоятельно или при незначительной коррекции преподавателем.

«3» (удовлетворительно): студент демонстрирует неглубокие теоретические знания, проявляет слабо сформированные навыки анализа явлений и процессов, недостаточное умение делать аргументированные выводы и приводить примеры, показывает недостаточно свободное владение монологической речью, терминологией, логичностью и последовательностью изложения, делает ошибки, которые может исправить только при коррекции преподавателем.

«2» (неудовлетворительно): студент демонстрирует незнание теоретических основ предмета, не умеет делать аргументированные выводы и приводить примеры, показывает слабое владение монологической речью, не владеет терминологией, проявляет отсутствие логичности и последовательностью изложения, делает ошибки, которые не может исправить даже при коррекции преподавателем, отказывается отвечать на занятии.