


ФГБОУ ВО НОВОСИБИРСКИЙ ГАУ
Кафедра информационных технологий и моделирования

Рег. № ПЧ.03-39
«05» 10 2022г.

УТВЕРЖДЕН
на заседании кафедры
Протокол от «23» 09 2022г. № 2
Заведующий кафедрой информационных
технологий и моделирования
 О.В. Агафонова
(подпись)

ФОНД
ОЦЕНОЧНЫХ СРЕДСТВ

Б1.В.09 Информационная безопасность
Шифр и наименование дисциплины

09.03.03 Прикладная информатика
Код и наименование направления подготовки

Прикладная информатика
Направленность (профиль)

Новосибирск 2022

Паспорт фонда оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Ведение в информационную безопасность	ПК-2 ПК-5	Кейс-задачи.
2	Информация с ограниченным доступом (тайны)	ПК-2 ПК-5	Перечень дискуссионных вопросов для семинара.
3	Нормативное регулирование информационной безопасности	ПК-2 ПК-5	Перечень тем устных сообщений для семинара
4	Лицензирование, аттестация, сертификация информационной безопасности	ПК-2 ПК-5	Кейс-задачи
5	Моделирование угроз информационной безопасности	ПК-2 ПК-5	Кейс-задачи
6	Теоретические основы криптографии, симметричные криптосистемы	ПК-2 ПК-5	Кейс-задача
7	Ассиметричные криптосистемы	ПК-2 ПК-5	Кейс-задача
	Контрольная работа, экзамен	ПК-2 ПК-5	Темы контрольной работы, вопросы к зачету

Кейс-задачи

Тема 1. Ведение в информационную безопасность.

Задание 1. Ответственность за нарушения законодательства прописана в Федеральных Законах и Кодексах (Административном, Уголовном и других). В рамках УК РФ, а именно раздела "Преступления против общественной безопасности и общественного порядка" главы 28 "Преступления в сфере компьютерной информации" описана ответственность за неправомерный доступ к охраняемой законом компьютерной информации (обратите внимание: именно компьютерной - в той же статье вы найдёте определение этого термина), если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Вопрос: какова ответственность за это деяние и от чего она зависит?

Задание 2. В результате утечки данных о клиентах одного из банков в руках злоумышленника оказались ФИО и номера телефонов клиентов. Воспользовавшись данной информацией, злоумышленник позвонил одному из клиентов банка и, представившись сотрудником банка, узнал данные для входа в интернет-банк. Это позволило ему войти в интернет-банк с учётными данными клиента, но попытка перевода средств на собственные счета (с карты клиента на счета злоумышленника) была заблокирована системой, при этом карта и учётная запись клиента остались функционирующими (не были заблокированы).

Ответьте на вопрос: были ли при этом нарушены конфиденциальность, целостность или доступность информации?

Предоставьте ответ в формате: была нарушена XXX, потому что ... (где вместо XXX - конфиденциальность, доступность или целостность, а ... - пояснение, например "потому что теперь клиент не может получить доступ к собственному счёту").

Обратите внимание, что может быть нарушено может быть не только одно свойство (назовём их так) информации.

Приведите ответ в свободной форме со своим комментарием.

Критерии оценки:

- оценка «зачтено» выставляется студенту, если задачи решены;
- оценка «не зачтено» выставляется студенту, если задачи не решены.

Перечень дискуссионных вопросов.

Тема 2. Информация с ограниченным доступом (тайны).

Вопросы:

1. Чем допуск к государственной тайне отличается от доступа к сведениям, составляющим государственную тайну?

2. Какие степени секретности выделяются в рамках государственной тайны?

3. Что такое "гриф секретности" и чем он отличается от степени секретности?

Закон о государственной тайне.

4. Что такое коммерческая тайна?

5. Какие меры по охране информации должны быть приняты в отношении коммерческой тайны?

6. Какие грифы можно использовать для носителей, содержащих информацию, составляющую коммерческую тайну? Должна ли быть указана ещё какая-либо информация?

Закон о коммерческой тайне

7. Что такое персональные данные?

8. Какие данные должно включать в себя согласие в письменной форме субъекта ПДн на обработку его ПДн?

9. В каком случае оператор вправе продолжить обработку ПДн даже при отзыве согласия на обработку ПДн со стороны субъекта ПДн?

Закон о персональных данных.

Критерии оценки:

- оценка «отлично» выставляется студенту, если сообщение выдержано студентом в рамках установленного регламента, структура доклада четко выражена, грамотно оформлен раздаточный материал. Студент демонстрирует свободное владение материалом, развернуто и аргументированно отвечает на дополнительные вопросы по теме сообщения;

- оценка «хорошо» - сообщение выдержано студентом в рамках установленного регламента, структура доклада четко выражена, грамотно оформлен раздаточный материал. Студент демонстрирует свободное владение материалом, развернуто отвечает на дополнительные вопросы по теме сообщения, но не всегда точно и аргументированно;

- оценка «удовлетворительно» - сообщение выдержано студентом в рамках установленного регламента, структура доклада выражена нечетко, недостаточно наглядно оформлен раздаточный материал. Студент недостаточно свободно владеет материалом, на дополнительные вопросы по теме сообщения отвечает не достаточно полно, демонстрируя фрагментарные, поверхностные знания содержания рассматриваемой темы;

- оценка «неудовлетворительно» - сообщение не выдержано студентом в рамках установленного регламента, структура доклада выражена нечетко, отсутствует раздаточный материал. Студент недостаточно свободно владеет

материалом. При ответе на дополнительные вопросы по теме сообщения демонстрирует незнание, либо отрывочное представление о данных вопросах материала; неумение использовать понятийный аппарат; отсутствие логической связи в ответе.

Перечень тем устных сообщений для семинара.

Тема 3. Нормативное регулирование информационной безопасности.

1. Сколько классов АС существует? Исходя из чего производится разделение АС на классы?
2. Сколько классов защищённости ГИС существует? Какой класс является самым высоким (наибольшее количество требований)?
3. Сколько уровней защищённости ПДн существует? Какой уровень является самым высоким (наибольшее количество требований)?
4. Сколько классов ИСОП существует? Какой класс является самым высоким (наибольшее количество требований)?
5. Сколько категорий значимости объектов КИИ существует? Какая категория является самой высокой (наибольшее количество требований)?
6. Сколько классов защищённости АСУ существует? Какой класс является самым высоким (наибольшее количество требований)?

Критерии оценки:

- оценка «отлично» выставляется студенту, если ответ показывает глубокое и системное знание материала. Студент демонстрирует отчетливое и свободное владение научным языком и терминологией. Логически корректное и убедительное изложение ответа.

- оценка «хорошо» - знание узловых проблем и основного содержания лекционного курса; умение пользоваться концептуально-понятийным аппаратом в процессе анализа основных проблем в рамках данной темы. В целом логически корректное, но не всегда точное и аргументированное изложение ответа.

- оценка «удовлетворительно» - фрагментарные, поверхностные знания содержания лекционного курса; затруднения с использованием научно-понятийного аппарата и терминологии; частичные затруднения с выполнением заданий;

- оценка «неудовлетворительно» - незнание, либо отрывочное представление о данных вопросах материала; неумение использовать понятийный аппарат; отсутствие логической связи в ответе.

Кейс-задачи

Тема 4. Лицензирование, аттестация, сертификация информационной безопасности.

Задача №1 Сертификация

Что такое сертификация? Укажите нормативный документ, в котором дано определение этого термина и сам термин. Какие три ключевые системы сертификации существуют и в каком документе об этом сказано? Сколько уровней доверия существует? Профили защиты на какие СЗИ уже существуют и опубликованы на сайте ФСТЭК?

Задача №2 Уровни доверия

СЗИ, соответствующие какому уровню доверия должны применяться в: ГИС 1 класса защищённости? ЗОКИИ 3 категории значимости? АС, содержащие сведения, составляющие гос.тайну? АСУ ТП 2 класса защищённости? ИСПДн 2 уровня защищённости?

Критерии оценки:

- оценка «зачтено» выставляется студенту, если задачи решены;
- оценка «не зачтено» выставляется студенту, если задачи не решены.

Кейс-задачи

Тема 5. Моделирование угроз информационной безопасности.

Посмотрите видео о том, как устроена система безопасности в дата-центрах Google (<https://www.youtube.com/watch?v=cLory3qLoY8>), опишите возможные модели угроз информационной безопасности? А так же средства, методы и технологии, применяемые для их защиты в компании?

Критерии оценки:

- оценка «зачтено» выставляется студенту, если задачи решены;
- оценка «не зачтено» выставляется студенту, если задачи не решены.

Кейс-задача

Тема 6. Теоретические основы криптографии, симметричные криптосистемы.

Задача:

Каким-то образом у вас оказался хэш пароля. Вот такой:
5693299e0bbe87f327caa802008af432fbe837976b1232f8982d3e101b5b6fab.

Вам нужно попробовать по длине хэша угадать его тип .

#	Name	Category
900	MD4	Raw Hash
0	MD5	Raw Hash
100	SHA1	Raw Hash
1300	SHA2-224	Raw Hash
1400	SHA2-256	Raw Hash
10800	SHA2-384	Raw Hash
1700	SHA2-512	Raw Hash
11700	GOST R 34.11-2012 (Streebog) 256-bit, big-endian	Raw Hash
11800	GOST R 34.11-2012 (Streebog) 512-bit, big-endian	Raw Hash
6900	GOST R 34.11-94	Raw Hash

Набор файлов с распространёнными паролями вы можете найти по адресу

<https://github.com/danielmiessler/SecLists/tree/master/Passwords/Common-Credentials>.

В качестве ответа необходимо прописать код, название функции хэширования и "угаданный" пароль.

Критерии оценки:

- оценка «зачтено» выставляется студенту, если задача решена;
- оценка «не зачтено» выставляется студенту, если задача не решена.

Кейс-задача

Тема 7. Ассиметричные криптосистемы.

Шифровать данные с помощью публичного ключа и расшифровывать с помощью приватного.

1. Создайте закрытый ключ с длиной 2048.
2. Сгенерируйте открытый ключ на базе закрытого.
3. Создайте файл message.txt со своей фамилией.
4. Зашифруйте сообщение с помощью публичного ключа.
5. Убедитесь, что файл _____.txt расшифровывается.

В качестве результата ответа:

Создайте два текстовых файла, где в первом будет прописан полный код шифрования, а во втором:

- Публичный и приватный ключ (public.key и private.key)
- Passphrase (строкой)
- Зашифрованный файл (cypher.txt)

Критерии оценки:

- оценка «зачтено» выставляется студенту, если задача решена;
- оценка «не зачтено» выставляется студенту, если задача не решена.

Темы контрольной работы

1. Разработка организационно-технических рекомендаций по повышению эффективности защиты конфиденциальной информации предприятия.
2. Разработка организационно-технических мер по защите информации, составляющей служебную тайну, предприятия.
3. Разработка предложений по созданию системы защиты информации предприятия централизованной структуры.
4. Разработка предложений по созданию защищенной информационной системы предприятия децентрализованной структуры.
5. Обоснование решений по определению способов оценки угроз информационной безопасности предприятия.
6. Разработка организационно-технических мер защиты выделенного помещения предприятия.
7. Разработка рекомендаций руководителю предприятия по оборудованию помещения для проведения служебных совещаний.
8. Разработка рекомендаций руководителю предприятия по оборудованию помещения для обработки персональных данных.
9. Системный анализ информационной инфраструктуры и разработка защищенной корпоративной информационной системы предприятия.
10. Разработка модели комплексной системы защиты информации предприятия.
11. Оценка рисков и управление информационной безопасностью предприятия.
12. Разработка автоматизированной системы оценки информационных рисков предприятия.
13. Организация комплексной системы защиты конфиденциальной информации предприятия.
14. Разработка политики информационной безопасности на основе анализа информационных рисков предприятия.
15. Совершенствование нормативно-методической базы защиты конфиденциальной информации предприятия.
16. Разработка организационно-технических мер противодействия утечке информации по техническим каналам предприятия.
17. Разработка рекомендаций по совершенствованию защиты коммерческой тайны предприятия.
18. Разработка рекомендаций по совершенствованию защиты ресурсов автоматизированной системы предприятия.
19. Оценка эффективности системы защиты информации предприятия.
20. Разработка рекомендаций по проведению аудита информационной безопасности предприятия.

Критерии оценки:

- оценка «зачтено» выставляется студенту, если выполнены все требования к написанию и защите контрольной работы: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы. Работа может быть зачтена и в том случае, когда основные требования к контрольной работе и ее защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём контрольной работы; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы;

- оценка «не зачтено» – тема контрольной работы не раскрыта, задания не выполнены, обнаруживается существенное непонимание проблемы.

Вопросов к экзамену

1. Информационная безопасность, субъекты и объекты, свойства.
2. Правовая система РФ.
3. Базовые термины в ИБ.
4. Закон о государственной тайне РФ.
5. Закон о коммерческой тайне РФ.
6. Закон о персональных данных РФ.
7. Закон о банка и банковской деятельности РФ.
8. Закон о связи РФ.
9. ФСТЭК России.
10. ГОСТ Р 50922-2006 и его роль в ИБ.
11. Техническое регулирование и лицензирование.
12. Лицензирование.
13. Аттестация.
14. Сертификация.
15. Уровни доверия.
16. Моделирование угроз, подходы.
17. Методика оценки угроз ФСТЭК (2021).
18. Моделирование угроз 1 этап: Определение негативных последствий.
19. Моделирование угроз 2 этап: Определение объектов воздействия.
20. Моделирование угроз 3.1 этап: Определение источников угроз.
21. Моделирование угроз 3.2 этап: Определение способов реализации угроз.
22. Моделирование угроз 3.3 этап: Оценка актуальности угроз.
23. Хранение информации.
24. История криптографии. Основы криптографии.
25. Симметричное шифрование.
26. Хэширование.
27. Асимметричные криптосистемы.
28. Электронная подпись.
29. Инфраструктура с открытым ключом.
30. Нормативное регулирование криптографии.

Критерии оценки:

– отметка **«отлично»** выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.

– отметка **«хорошо»** выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных

неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.

– отметка **«удовлетворительно»** выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, демонстрирует недостаточно систематизированные теоретические знания программного материала, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.

– отметка **«неудовлетворительно»** выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки при его изложении, неуверенно, с большими затруднениями выполняет практические работы.

ЗАДАНИЯ ДЛЯ ОЦЕНКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Задания для оценки сформированности компетенции ПК-2:

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- а. Разработка аппаратных средств обеспечения правовых данных
- б. Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- в. Разработка и конкретизация правовых нормативных актов обеспечения безопасности

Ответ – в

2) Виды информационной безопасности:

- а. Персональная, корпоративная, государственная
- б. Клиентская, серверная, сетевая
- в. Локальная, глобальная, смешанная

Ответ – а

3) Основные объекты информационной безопасности:

- а. Компьютерные сети, базы данных
- б. Информационные системы, психологическое состояние пользователей
- в. Бизнес-ориентированные, коммерческие системы

Ответ - а

4) К основным функциям системы безопасности можно отнести все перечисленное:

- а. Установление регламента, аудит системы, выявление рисков
- б. Установка новых офисных приложений, смена хостинг-компании
- в. Внедрение аутентификации, проверки контактных данных пользователей

Ответ – а

5) Свойством информации, при обеспечении информационной безопасности является:

- а. Целостность
- б. Достоверность
- в. Актуальность

Ответ – а

6) ЭЦП – это:

Ответ ...

7) Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

Ответ ...

8) Какие свойства информации рассматриваются в разрезе информационной безопасности?

Ответ ...

9) Естественные угрозы безопасности информации вызваны:

Ответ ...

10) Фишинг – это

Ответ ...

Задания для оценки сформированности компетенции ПК-5:

1) Когда получен спам по e-mail с приложенным файлом, следует:

а. Прочитать приложение, если оно не содержит ничего ценного – удалить.

б. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама.

в. Удалить письмо с приложением, не раскрывая (не читая) его.

Ответ в

2) Наиболее распространены угрозы информационной безопасности корпоративной системы:

а. Покупка нелегального ПО.

б. Ошибки эксплуатации и неумышленного изменения режима работы системы

в. Сознательного внедрения сетевых вирусов.

Ответ - б

3) Утечкой информации в системе называется ситуация, характеризующаяся:

а. Потерей данных в системе

б. Изменением формы информации

в. Изменением содержания информации

Ответ – а

4) Системой криптографической защиты информации является:

а. CAuditPro

б. BFoxPro

в. VeraCrypt

Ответ - в

5) К внутренним нарушителям информационной безопасности относится:

- а. клиенты;
- б. посетители;
- в. технический персонал, обслуживающий здание

Ответ – в

6) Конфиденциальная информация это ...

Ответ ...

7) Система защиты государственных секретов определяется Законом

Ответ ...

8) Документы, содержащие государственную тайну снабжаются грифами

Ответ ...

9) Конфиденциальность информации это

Ответ ...

10) Аутентификация это

Ответ ...

Критерии оценки результатов:

- оценка «отлично» выставляется студенту, если он отвечает верно на 80-100% вопросов.
- оценка «хорошо» выставляется студенту, если он отвечает верно на 70-79% вопросов.
- оценка «удовлетворительно» выставляется студенту, если он отвечает верно на 60-69% вопросов.
- оценка «неудовлетворительно» выставляется студенту, если он не освоил материал темы, дает менее 60% правильных ответов.

МАТРИЦА СООТВЕТСТВИЯ КРИТЕРИЕВ ОЦЕНКИ УРОВНЮ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Критерии оценки	Уровень сформированности компетенций
Оценка по пятибалльной системе	
«Отлично»	«Высокий уровень»
«Хорошо»	«Повышенный уровень»
«Удовлетворительно»	«Пороговый уровень»
«Неудовлетворительно»	«Не достаточный»
Оценка по системе «зачет – незачет»	
«Зачтено»	«Достаточный»
«Не зачтено»	«Не достаточный»

Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1. Положение «О балльно-рейтинговой системе аттестации студентов»: СМК ПНД 08-01-2022, введено приказом от 28.09.2011 №371-О (<http://nsau.edu.ru/file/403>: режим доступа свободный);

2. Положение «О проведении текущего контроля и промежуточной аттестации обучающихся в ФГБОУ ВО Новосибирский ГАУ»: СМК ПНД 77-01-2022, введено в действие приказом от 03.08.2015 №268а-О (<http://nsau.edu.ru/file/104821>: режим доступа свободный).