Документ подписан простой электронной подписью
Информация о владельце:
ФИО: [illegible]ва Людмила Вячеславовна
Должность: Проректор по учебно-методической работе
Дата подписания: 09.11.2026 12:59:17
Уникальный программный ключ:
b066544bae1e449cd8bfce392f7224a676a271b2

о НАК(б) 26

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ЭКОНОМИКИ И ТОРГОВЛИ ИМЕНИ МИХАИЛА ТУГАН-БАРАНОВСКОГО»

Кафедра информационных систем и технологий управления

УТВЕРЖДАЮ
Заведующий кафедрой
информационных систем и технологий
управления
_____ В.О. Бессарабов
«10» февраля 2026 г.

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ УПРАВЛЕНИЯ

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по учебной дисциплине
Б1.В.16 «Информационная безопасность»
(шифр и наименование дисциплины)

38.03.01 Экономика
(код и наименование направления подготовки)

Цифровая аналитика и контроль
(наименование профиля подготовки)

Разработчик:
Доцент _____ Н.С. Пальчикова
(должность)

Оценочные материалы рассмотрены и утверждены на заседании кафедры
от «10» февраля 2026 г., протокол № 15

Донецк 2026 г.

Паспорт
оценочных материалов по дисциплине
«Информационная безопасность»

Перечень компетенций, формируемых в результате освоения учебной дисциплины (модуля)

№ п/п	Код контролируемой компетенции	Формулировка контролируемой компетенции	Контролируемые разделы (темы) дисциплины (модуля)	Этапы формирования (семестр изучения)
1.	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Тема 1. Введение в информационную безопасность. Модели информационной безопасности. Тема 2. Выявление возможных нарушений и атак в экономических информационных системах (ЭИС). Тема 3. Противодействие вредоносным программам в ЭИС. Тема 4. Применение криптографических систем шифрования данных. Тема 5. Методы защиты информации в корпоративных вычислительных сетях (Интранет). Тема 6. Методы защиты информации в глобальной сети Интернет. Тема 7. Аудит информационной безопасности. Тема 8. Анализ информационных рисков.	4

Показатели и критерии оценивания компетенций, описание шкал оценивания

Таблица 2 – Показатели оценивания компетенций

№ п/п	Код контролируемой компетенции	Показатель оценивания (знания, умения, навыки)	Контролируемые разделы (темы) дисциплины (модуля)	Наименование оценочного средства
1.	УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	ИД-1 Определяет связи между поставленными задачами и ожидаемые результаты их решения	Тема 1. Введение в информационную безопасность. Модели информационной безопасности. Тема 2. Выявление возможных нарушений и атак в экономических информационных системах (ЭИС).	Собеседование, тест, индивидуальное задание
		ИД-2 В рамках поставленных задач определяет имеющиеся ресурсы и ограничения, действующие правовые нормы	Тема 3. Противодействие вредоносным программам в ЭИС. Тема 4. Применение криптографических систем шифрования данных. Тема 5. Методы защиты информации в корпоративных вычислительных сетях (Интранет). Тема 6. Методы защиты информации в глобальной сети Интернет. Тема 7. Аудит информационной безопасности. Тема 8. Анализ информационных рисков.	

Критерии и шкала оценивания по оценочному материалу «Тест» по темам смысловых модулей 1-2

Шкала оценивания (интервал баллов)	Критерии оценивания
10	Процент правильных ответов составляет 95-100%
9	Процент правильных ответов составляет 85-90%
8	Процент правильных ответов составляет 71-80%
7	Процент правильных ответов составляет 61-70%
6	Процент правильных ответов составляет 51-60%
5	Процент правильных ответов составляет 41-50%
4	Процент правильных ответов составляет 31-40%
3	Процент правильных ответов составляет 21-30%
2	Процент правильных ответов составляет 16-20%
1	Процент правильных ответов составляет 10-15%
0	Процент правильных ответов составляет 0-10%

Критерии и шкала оценивания по оценочному материалу «Практическая работа» по темам 1,2,3,4

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Практическая работа выполнена на высоком уровне, допущены незначительные ошибки при выполнении, обучающийся аргументировано и уверенно ответил на вопросы преподавателя
3-4	Практическая работа выполнена на среднем уровне, допущены более 2 незначительные ошибки при расчетах или оформлении, обучающийся ответил на большинство вопросов преподавателя
1-2	Практическая работа выполнена на низком уровне, допущено большое количество существенных ошибок, обучающийся неуверенно ответил на вопросы преподавателя
0	Практическая работа не выполнена

Критерии и шкала оценивания по оценочному материалу «Практическая работа» по теме 5

Шкала оценивания (интервал баллов)	Критерий оценивания
30	Практическая работа выполнена на высоком уровне, допущены незначительные ошибки при выполнении, обучающийся аргументировано и уверенно ответил на вопросы преподавателя
20	Практическая работа выполнена на среднем уровне, допущены более 2 незначительные ошибки при расчетах или оформлении, обучающийся ответил на большинство вопросов преподавателя
5-10	Практическая работа выполнена на низком уровне, допущено большое количество существенных ошибок, обучающийся неуверенно ответил на вопросы преподавателя
0	Практическая работа не выполнена

Критерии и шкала оценивания по оценочному материалу «Практическая работа» по теме 8

Шкала оценивания (интервал баллов)	Критерий оценивания
20	Практическая работа выполнена на высоком уровне, допущены незначительные ошибки при выполнении, обучающийся аргументировано и уверенно ответил на вопросы преподавателя
10-15	Практическая работа выполнена на среднем уровне, допущены более 2 незначительные ошибки при расчетах или оформлении, обучающийся ответил на большинство вопросов преподавателя
5-10	Практическая работа выполнена на низком уровне, допущено большое количество существенных ошибок, обучающийся неуверенно ответил на вопросы преподавателя
0	Практическая работа не выполнена

Примерный перечень оценочных материалов

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	**2**	**3**	**4**
1	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий
2	Практическая работа	Средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по темам дисциплины с использованием соответствующего программного обеспечения.	Комплект индивидуальных заданий для выполнения практической работы

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков

При изучении учебной дисциплины в течение семестра студент максимально может набрать 100 баллов. Минимальное количество баллов, необходимое для получения зачета составляет 60 баллов.

Текущий контроль знаний обучающихся осуществляется на основании оценки систематичности и активности по каждой теме программного материала учебной дисциплины.

Текущий контроль знаний обучающихся осуществляется с помощью оценки докладов, выполнения практических работ, тестов.

Доклад обучающегося должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения, правила в конкретных случаях.

Выполнение обучающимся практических работ направлено на:

- обобщение, систематизацию, углубление, закрепление полученных теоретических знаний по конкретным темам учебной дисциплины;
- формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности;
- развитие интеллектуальных аналитических умений обучающихся;
- выработку при решении практических работ таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.

Практические работы предполагают выполнение индивидуальных заданий разного уровня, расчет и анализ различных показателей, их визуальное представление, составление и анализ формул, уравнений, обработка результатов проведенных расчетов.

Тестирование по темам смысловых модулей может проводиться в компьютерных классах с помощью программы «Тесты» согласно графика проведения текущего модульного контроля, а также в системе дистанционного обучения Moodle.

Промежуточная аттестация осуществляется в форме дифференцированного зачета.

Относительно распределения баллов на итоговом контроле оценки знаний, умений и навыков обучающихся по результатам выполнения заданий используется следующая шкала оценивания:

46-60 баллов выставляется в случае полного качественного выполнения всех заданий или при наличии одной или двух незначительных ошибок в вычислении, решение четкое и обоснованное, использования творческих подходов;

36-45 баллов выставляется тогда, когда обучающийся показал способность к применению изученного материала к решению задач; объяснения и обоснования полностью соответствуют требованиям программы дисциплины, но являются недостаточными; четкое оформление решения задач; решение содержит одну или две несущественные ошибки;

20-35 баллов выставляется, если обучающийся овладел навыками решения стандартных задач, умением проводить аналитические расчеты, но решение задач содержит большое количество существенных ошибок;

0-19 баллов выставляется в случае, когда ни одно из заданий не выполнено или их решение содержит очень большое количество существенных ошибок; обучающийся не показал владение теоретическими знаниями и приемами решения задач.

Опираясь на знания обучающихся, преподаватель оставляет за собой право решающего слова во время оценивания знаний.

Система оценивания по дисциплине по очной форме обучения*

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль:		
- тестирование (темы смысловых модулей 1,2,3)	10	30
- практическая работа (тема 1,2,3,4)	10	40
- практическая работа (тема 5)	20	20
- практическая работа (тема 8)	10	10
Промежуточная аттестация	*зачет*	*100*
Итого за семестр	*100*	

* в соответствии с утвержденными оценочными материалами по дисциплине

Система оценивания по дисциплине на очно-заочной форме обучения

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль:		
- тестирование (темы смыслового модулей 1)	10	10
- тестирование (темы смыслового модуля 2)	10	10
- тестирование (темы смыслового модуля 3)	10	10
- контрольная работа (тема 5,8)	35	70
Промежуточная аттестация	зачет	100
Итого за семестр	100	

РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Максимальное количество баллов за текущий контроль и самостоятельную работу								**Максимальная сумма баллов**		
Смысловой модуль № 1		**Смысловой модуль № 2**				**Смысловой модуль № 3**		**Текущий контроль**	**Зачет**	**Все виды учебной деятельности**
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	100	100	100
10	20	10	10	20	10	10	10			

Т1 ... Т8 – номера тем соответствующих смысловых модулей

Государственная шкала оценивания академической успеваемости

Сумма баллов за все виды учебной деятельности	По государственнойшкале
90-100	5 «отлично» / «зачтено»
75-89	4 «хорошо» / «зачтено»
60-74	3 «удовлетворительно» / «зачтено»
Менее 60	2 «неудовлетворительно» / «не зачтено»

Таблица 3– Критерии и шкала оценивания по оценочному средству «Собеседование»

Шкала оценивания (интервал баллов)	Критерии оценивания
5	Собеседование пройдено на высоком уровне (студент ответил на все вопросы преподавателя, владеет профильным понятийным аппаратом)
3-4	Собеседование пройдено на среднем уровне (студент в целом ориентируется в учебном материале, отвечает на вопросы, допустив некоторые неточности)
1-2	Собеседование пройдено на низком уровне (при ответе на вопросы преподавателя студент допускает существенные неточности, не владеет в достаточной степени профильным категориальным аппаратом
0	Собеседование не пройдено (студент не готов, на вопросы не отвечает.)

Таблица 4– Критерии и шкала оценивания по оценочному средству «Индивидуальное задание»

Шкала оценивания (интервал баллов)	Критерии оценивания
5	Индивидуальное задание выполнено на высоком уровне, допущены 1-2 незначительные ошибки при расчетах или оформлении, студент аргументировано и уверенно ответил на вопросы преподавателя
3-4	Индивидуальное задание выполнено на среднем уровне, допущены более 2 незначительные ошибки при расчетах или оформлении, студент ответил на большинство вопросов преподавателя
1-2	Индивидуальное задание выполнено на низком уровне, допущено большое количество существенных ошибок, студент неуверенно ответил на вопросы преподавателя
0	Индивидуальное задание не выполнено

Таблица 5 – Критерии и шкала оценивания по оценочному средству «Тест»

Шкала оценивания (интервал баллов)	Критерии оценивания
9-10	Процент правильных ответов составляет 90-100%
7-8	Процент правильных ответов составляет 75-89%
5-6	Процент правильных ответов составляет 60-74%
3-5	Процент правильных ответов составляет 35-59%
0-2	Процент правильных ответов составляет 0-35%

Таблица 6–Перечень оценочных средств

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	Собеседование (устный или письменный опрос)	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой учебной дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по учебной дисциплине или определенному разделу, теме, проблеме и т.п.	Вопросы по темам учебной дисциплины
2.	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий
3.	Индивидуальное задание	Средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по темам дисциплины с использованием соответствующего программного обеспечения.	Комплект индивидуальных заданий для выполнения практической работы

Смысловой модуль 1. Информационная безопасность в экономических информационных системах.

Контрольные вопросы для проведения собеседования по теме «Введение в информационную безопасность. Модели информационной безопасности».

1.Что такое информационная безопасность?
2.Перечислите основные угрозы информационной безопасности.
3.Какие существуют модели информационной безопасности?
4.Какие методы защиты информации выделяют?
5.Что такое правовые методы защиты информации?
6.Что такое организационные методы защиты информации?
7.Что такое технические методы защиты информации?
8.Что такое программно-аппаратные методы защиты информации?
9.Что такое криптографические методы защиты информации?
10.Что такое физические методы защиты информации?
11.Какие главные государственные органы в области обеспечения информационной безопасности?
12.Перечислите виды защищаемой информации.

Индивидуальное задание по теме по теме «Введение в информационную безопасность. Модели информационной безопасности».

Составить досье на одногруппника с использованием Интернет-ресурсов для оценки воздействия ИКТ-технологий на неприкосновенность частной жизни; оценить угрозу злоумышленного применения информации и выработать рекомендации по обеспечению необходимого уровня безопасности частной жизни в мире цифровых зависимостей.

Контрольные вопросы для проведения собеседования по теме «Выявление возможных нарушений и атак в экономических информационных системах (ЭИС)»

1. Понятие угрозы информационной системы
2. Понятие уязвимости информационной системы
3. Классификация угроз ЭИС

4. Виды уязвимостей ЭИС
5. Классификация компьютерных преступлений

Индивидуальное задание по теме «Выявление возможных нарушений и атак в экономических информационных системах (ЭИС)»

Составить кроссворд из 15 слов, которые включают виды угроз и уязвимостей ЭИС, а также основные понятия дисциплины «Информационная безопасность».

Примеры тестовых заданий по смысловому модулю 1

1. Информация - это

А) это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

Б) совокупность некоторых знаков, символов, сигналов;

В) отдельные документы и отдельные массивы документов.

2. Защищаемая информация - это

А) совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала;

Б) информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственниками информации;

В) это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

3. Система обработки информации - это

А) совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов;

Б) отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах;

В) совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации.

4. Объект информатизации - это

А) совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов;

Б) информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственниками информации;

В) совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

5. Выделяются следующие направления защиты информации:

А) правовая защита информации;

Б) техническая защита информации;

В) криптографическая защита информации;

Г) физическая защита информации;

Д) математическая защита информации.

6. Средство защиты информации - это

А) техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации;

Б) средства контроля эффективности защиты информации;

В) средства физической защиты информации;

Г) криптографические средства защиты информации.

7. Этапы развития информационной безопасности:

А) 1816, 1816, 1935, 1946, 1965, 1973, 1985;

Б) 1745,1863,1935,1965,1970,1973,1985;

В) 1815,1817,1934,1945,1966,1974,1989;

Г) 1812,1816,1931,1941,1960,1971,1981.

8. Основными задачами системы ИБ являются:

А) своевременное выявление и устранение угроз безопасности и ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба интересам субъектов информационных отношений;

Б) актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения;

В) создание механизма и условий оперативного реагирования на угрозы безопасности и проявлению негативных тенденций в функционировании предприятия;

Г) эффективное пресечение посягательств на ресурсы и угроз персоналу на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;

Д) создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности на достижение целей организации.

9. Основу мандатной политики безопасности составляет мандатное управление доступом, которое подразумевает, что:

А) все субъекты и объекты должны быть идентифицированы, задан линейно упорядоченный набор меток секретности;

Б) каждому объекту системы присвоена метка секретности, определяющая ценность содержащейся в нем информации - его уровень секретности;

В) каждому субъекту системы присвоена метка секретности, определяющая уровень доверия к нему - его уровень доступа;

Г) решение о разрешении доступа субъекта к объекту принимается исходя из типа доступа и сравнения метки субъекта и объекта.

10. Уязвимость - это

А) это присущие объекту ЭИС причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта ИС, свойствами архитектуры ЭИС, протоколами обмена и интерфейсами, применяемым программным обеспечением и аппаратной платформы, условиями эксплуатации, невнимательностью сотрудников

Б) это возможные действия реализации угрозы при взаимодействии источника угрозы через имеющиеся уязвимости

В) это потенциальные антропогенные, техногенные и стихийные угрозы безопасности

Смысловой модуль 2. Инструменты защиты информации в экономических информационных системах.

Контрольные вопросы для проведения собеседования по теме «Противодействие вредоносным программам в ЭИС»

1. Какие виды компьютерных угроз существуют?

2.Что такое брандмауэр?

3.Что такое антивирусная программа?

4.Что такое эвристический алгоритм поиска вирусов?

5.Что такое сигнатурный поиск вирусов?

6.Методы противодействия сниффингу?

7.Какие программные реализации программно-аппаратных средств защиты информации вы знаете?

8.Что такое механизм контроля и разграничения доступа?

9.Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?

10.Что такое средства стенографической защиты информации?

Индивидуальное задание по теме «Противодействие вредоносным программам в ЭИС»

Подготовить на основе данных сайта www.anti-malware.ru, раздел Тесты - Рейтинги антивирусов (https://www.anti-malware.ru/tests_history), доклад про антивирус (историю создания и использования, количество наград и проваленных тестов), доказать почему выбранный антивирус является наилучшим.

Контрольные вопросы для проведения собеседования по теме «Применение криптографических систем шифрования данных»

1.Что такое криптография?

2.Какие используются симметричные алгоритмы шифрования?

3.Какие используются ассиметричные алгоритмы шифрования?

4.Что такое криптографическая хеш-функция?

5.Какие используются криптографические хеш-функции?

6.Что такое цифровая подпись?

7.Что такое инфраструктура открытых ключей?

8.Какие российские и международные стандарты на формирование цифровой подписи существуют?

9.Какие основные криптографические протоколы используются в сетях?

Индивидуальное задание по теме «Применение криптографических систем шифрования данных»

Зашифровать свое ФИО используя методы одиночной перестановки, двойной перестановки магического квадрата и шифра простой замены.

Контрольные вопросы для проведения собеседования по теме «Методы защиты информации в корпоративных вычислительных сетях (Интранет)»

1. Идентификация и аутентификация.
2. Группы методов аутентификации.
3. Понятие учетной записи пользователя.
4. Особенности администрирования парольной системы, использующей многоразовые пароли.
5. Приемы обхода парольной защиты и методы противодействия им.
6. Перебор в ограниченном диапазоне.
7. Понятие социального инжиниринга.
8. Фишинг. Примеры применения.
9. Понятие токена.
10. Управление доступом.

Индивидуальное задание по теме «Методы защиты информации в корпоративных вычислительных сетях (Интранет)»

1. Организовать парольную защиту файлов средствами текстового редактора
2. Организовать защиту файлов средствами электронной таблицы.
3. Организовать парольную защиту баз данных.

Сводная ведомость начисления квартальной премии №___
за _____ квартал _____года

Табельный номер	*ФИО сотрудника*	*Код должности*	*Должность*	*Сумма заключенных контрактов*	*К выплате*
1		2	Менеджер		*
2		1	Руководитель		*
3		4	Ассистент		*
4		3	Аналитик		*
…		…	…		*
15		…	…		*
Премия			27%		

Дата создания ведомости_____

Главный бухгалтер_____ Руководитель _____

1. При организации парольной защиты файлов средствами текстового редактора:

1.1. Установите защиту документа от изменений так, чтобы изменения можно было вносить только в поля форм и в таблицу с фамилиями и другими данными сотрудников организации.

2. При организации защиты файлов средствами электронной таблицы:

2.1. Создайте лист **Должности**, содержащий данные: код должности, наименование должности, ФИО сотрудников с наибольшей суммой заключенных контрактов.

2.2. На листе **Статистика** создайте таблицу обработки данных, содержащихся на листах **Ведомость** и **Должности** таким образом, что при вводе в ячейку **B1** кода должности (1-4) в ячейках диапазона **B4:B9** появились следующие данные: наименование должности, ФИО сотрудника с наибольшей суммой заключенных контрактов, число сотрудников на аналогичной должности, размер общей и средней премии по должности.

3. При организации парольной защиты баз данных:

3.1. Создайте таблицу базы данных **Сотрудники**, выполнив импорт данных из именованного диапазона **Сотрудники** с листа **Ведомость.**

3.2. Создайте таблицу **Должности**, импортировав данные о должностях из именованного диапазона **Должности**. Ключевое поле таблицы – **Код должности**.

3.3. Установите связь между таблицами **Должности** и **Сотрудники** по полю **Код должности** (связь **один-ко-многим**).

3.4. Выполните статистическую обработку данных из таблиц **Сотрудники** и **Должности** по аналогии с обработкой данных, выполненной в п.2.2 (итоговый запрос).

Контрольные вопросы для проведения собеседования по теме «**Методы защиты информации в глобальной сети Интернет»**

1. Средства защиты сети.
2. Межсетевые экраны
3. Классификаций межсетевых экранов по различным критериям.
4. Виртуальные частные сети (VPN)
5. Системы обнаружения вторжений (IDS)

Примеры тестовых заданий по смысловому модулю 2

1. Асинхронная атака - это

А) используется как для анализа процессов, в которые преступники хотят вмешаться, так и для планирования методов совершения преступления

состоит в смешивании и одновременном выполнении компьютерной системой команд двух или нескольких пользователей;

Б) разновидность логической бомбы, которая срабатывает при достижении определенного момента времени;

В) использование компьютерных систем или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характера.

2. К интересующим нарушителя персональным данным пользователя атакуемого компьютера относятся:

А) хранящиеся в памяти компьютера документы и другие данные пользователя;

Б) имена учетных записей и пароли для доступа к различным сетевым ресурсам (системам электронных денег и платежей, Интернет-аукционам, Интернет-пейджерам, электронной почте, Интернет-сайтам и форумам, онлайн-играм);

В) адреса электронной почты других пользователей, 1Р-адреса других компьютеров сети.

3. После получения управления код вируса выполняет следующую последовательность действий:

А) заражение других файлов (комбинированные вирусы) и системных областей дисковой памяти;

Б) установка в оперативной памяти собственных резидентных модулей (резидентные вирусы);

В) выполнение других действий, зависящих от реализуемого вирусом алгоритма;

Г) продолжение обычной процедуры открытия файла (например, передача управления исходному коду зараженной программы).

4. При запуске зараженного файла управление получает код вируса, который:

А) устанавливает в оперативной памяти свой резидентный модуль, который в дальнейшем будет перехватывать все обращения к зараженному диску;

Б) загружает исходный программный файл и передает ему управление;

В) код программы реального режима процессора, которая получает управление при попытке запуска приложения в среде операционной системы MS-DOS.

5. Простейший макровирус в документе заражает остальные файлы документов следующим образом:

А) при открытии зараженного документа управление получает содержащийся в нем макрос с кодом вируса;

Б) вирус помещает в файл шаблонов normal.dot другие макросы со своим кодом (например, FileOpen, FileSaveAs и FileSave);

В) вирус устанавливает в реестре и (или) в инициализационном файле соответствующий флаг о произведенном заражении;

Г) при последующем запуске первым открываемым файлом фактически является уже зараженный файл шаблонов normal.dot, что позволяет коду вируса автоматически получать управление, а заражение других файлов документов может происходить при их сохранении с помощью стандартных команд.

6. Программной закладкой называют

А) внешнюю или внутреннюю по отношению к атакуемой компьютерной системе программу, обладающую определенными разрушительными функциями по отношению к этой системе;

Б) осуществление различных несанкционированных пользователем действий (сбор конфиденциальной информации и ее передачу нарушителю, разрушение или намеренную модификацию информации пользователя, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях ("троянские" программы или просто "троянцы");

В)уничтожение или внесение изменений в функционирование программного обеспечение КС, уничтожение или изменение обрабатываемых в ней данных после выполнения некоторого условия или получения некоторого сообщения извне КС ("логические бомбы");

Г) перехват паролей пользователей КС с помощью имитации приглашения к его вводу или перехвата всего ввода пользователей с клавиатуры.

7. Криптографией принято называть

А) науку о математических методах обеспечения конфиденциальности и аутентичности (целостности и подлинности) информации;

Б) способ скрытой передачи сообщений без сокрытия самого факта их передачи;

В) тайнопись.

8. Временная сложность - это

А) объем памяти, необходимой для хранения полученных в ходе работы данных, как функция от размера задачи;

Б) это время, затрачиваемое алгоритмом для решения задачи, рассматриваемое как функция от размера задачи

В) стойкость шифра к раскрытию методами криптоанализа

9. По типу преобразований шифры можно разделить на следующие группы:

А) шифры замены (подстановки);

Б) шифры перестановки;

В) шифры гаммирования;

Г) шифры на основе математических преобразований;

Д) шифры на основе аналитических преобразований.

10. По типу использования ключей шифры делятся на:

А) симметричные;

Б) асимметричные;

В) использующие для шифрования и расшифровывания два различных ключа;

Г) блочные;

Д) потоковые.

Смысловой модуль 3. Проверка состояния информационной безопасности в экономических информационных системах.

Контрольные вопросы для проведения собеседования по теме «Аудит информационной безопасности»

1. Протоколирование и аудит
2. Понятие подозрительной активности.
3. Основные задачи активного аудита.
4. Сигнатура атаки
5. Функциональные компоненты и архитектура активного аудита

Контрольные вопросы для проведения собеседования по теме «Анализ информационных рисков»

1. Понятие информационного риска
2. Методики анализа, оценки и управления рисками информационной безопасности
3. Методы оценки рисков информационной безопасности
4. Примеры использования метода CORAS.
5. Примеры использования метода OCTAVE.
6. Примеры использования матричного метода анализа.

Индивидуальное задание по теме «Анализ информационных рисков».

Используя ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий» произвести оценку рисков информационной безопасности на основании возможных потерь для организации в случае реализации угрозы.

Примеры тестовых заданий по смысловому модулю 3

1. Аудит информационной безопасности предприятия – это

А) сбор и накопление информации о событиях, происходящих в информационной системе;

Б) анализ накопленной информации, проводимый оперативно, в реальном времени или периодически;

В) процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности организации в соответствии с определенными критериями, стандартами и показателями.

2. Реализация протоколирования и аудита решает следующие задачи:

А) выявление нештатных ситуаций;

Б) обеспечение подотчетности пользователей и администраторов;

В) обеспечение возможности реконструкции последовательности событий;

Г) обнаружение попыток нарушений информационной безопасности;

Д) предоставление информации для выявления и анализа проблем.

3. Под подозрительной активностью понимается

А) активность, не соответствующая политике безопасности

поведение пользователя или компонента информационной системы, являющееся злоумышленным;

Б) совокупность условий, при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию;

В) действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику безопасности.

4. Сигнатура атаки - это

А) совокупность условий, при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию;

Б) зависимость от других средств безопасности;

В) описание изменений, внесенных в базы данных защиты;

Г) имена затронутых объектов.

5. Анализ информационных рисков - это

А) анализ осуществляющийся при помощи различных инструментов и методов формирования процессов защиты информации;

Б) это процесс совокупного оценивания степени защиты информационной системы с определением количественных;

В)автоматизация управления рисками, оптимизация финансовых расходов на управление, оптимизация времени на сопровождение систем безопасности компании, поддержка непрерывности бизнеса.

6. Наиболее известным подходом к количественному расчету информационных рисков является

А) AssetValue;

Б) ExposureFactor;

В) CRAMM;

Г) AnnualRateofOccurrence.

7. Оценка возможности возникновения угрозы:

А) AssetValue;

Б) ExposureFactor;

В) AnnualLossExposure;

Г) CRAMM.

8. Риск можно:

А) принять - согласиться с риском и понести обусловленные им потери;

Б) снизить - принять определенный перечень мер, направленный на минимизацию риска;

В) передать - возложить затраты на покрытие ущерба на страховую компанию, либо же - трансформировать риск в риск с более низким уровнем опасности с помощью специальных механизмов.

9. Методы оценки рисков информационной безопасности

А) Метод CORAS;

Б) Метод OCTAVE;

В) Operationally Critical Threat;

Г) Матричный метод анализа.