

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Крылова Людмила Владимировна
Должность: Проректор по учебно-методической работе
Дата подписания: 28.02.2025 22:53:41
Уникальный идентификатор документа:
b066544bae1e449cd8bfc39267224a676e271b2

0 СТДВР(с) 24

**МИНИСТЕРСТВО НАУКИ И
ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ
ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО
ОБРАЗОВАНИЯ «РОССИЙСКИЙ
ЭКОНОМИЧЕСКИЙ
УНИВЕРСИТЕТ
ИМЕНИ Г.В. ПЛЕХАНОВА»**

**МИНИСТЕРСТВО НАУКИ И
ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

Б1.О.15 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Специальность: 38.05.02 Таможенное дело

Специализация: Таможенные платежи и валютное регулирование

Уровень высшего образования: Специалитет

Год начала подготовки 2024

Составитель:

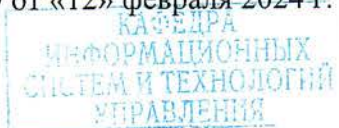
старший преподаватель кафедры

информационных систем и технологий управления

Н.С. Пальчикова

Оценочные материалы одобрены на заседании кафедры информационных систем и технологий управления Протокол №19 от «12» февраля 2024 г.

Заведующий кафедрой



В.О. Бессарабов

Паспорт

оценочных материалов по учебной дисциплине

«Информационная безопасность»

(наименование учебной дисциплины)

Таблица 1 – Перечень компетенций (элементов компетенций), формируемых в результате освоения учебной дисциплины (модуля)

№ п/п	Код контролируемой компетенции	Формулировка контролируемой компетенции	Контролируемые разделы (темы) учебной 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.	1

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) учебной дисциплины (модуля)	Наименование оценочного средства
1.	УК-1	УК-1.2. З-1. Знает методику проведения оценки адекватности и достоверности информации о проблемной ситуации, обнаружения признаков противоречивой информации, полученной из разных источников	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
		УК-1.2. У-1. Умеет осуществлять поиск решений проблемной ситуации на основе действий, эксперимента и опыта УК-1.2. У-2. Умеет критически оценивать возможные варианты решения проблемной ситуации на основе анализа причинно-следственных связей	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.	

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

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков

При изучении учебной дисциплины в течение семестра студент максимально может набрать 100 баллов.

Система оценивания всех видов работ по учебной дисциплине «Информационная безопасность» приведена в таблицах 3-5.

Текущий контроль знаний студентов осуществляется на основании оценки: систематичности и активности по каждой теме программного материала дисциплины; заинтересованного, выполнения индивидуальных заданий и своевременной их защиты.

Текущий контроль знаний студентов осуществляется с помощью тестов, проведения собеседования и защиты индивидуального задания при выполнении практической работы.

Для выполнения индивидуального задания студент должен пройти предварительную теоретическую и практическую подготовку на лекционных и практических занятиях, а также при самостоятельном изучении литературных источников. Индивидуальные задания выполняются студентом в компьютерных классах, распечатываются на листах формата А4 и оформляются в отчет. Отчет должен иметь титульный лист и выполненное индивидуальное задание согласно варианту, который соответствует номеру в общем списке группы. Студент представляет отчет преподавателю в бумажном и электронном варианте и защищает свою работу, отвечая на вопросы по теме работы. Отчет выполняется своевременно согласно календарно-тематическому плану учебной дисциплины (модуля) «Информатика».

Тестирование по темам смысловых модулей проводится в компьютерных классах с помощью программы «Тесты» согласно графику проведения модульного контроля.

Промежуточная аттестация осуществляется в форме экзамена. В таблице 7 приведена шкала оценивания

Таблица 7 – Соответствие государственной шкалы оценивания академической успеваемости

Сумма баллов за все виды учебной деятельности	По государственной шкале	Определение
90-100	«Отлично» (5)	отлично – отличное выполнение с незначительным количеством неточностей
80-89	«Хорошо» (4)	хорошо – в целом правильно выполненная работа с незначительным количеством ошибок (до 10 %)
75-79		хорошо – в целом правильно выполненная работа с незначительным количеством ошибок (до 15 %)
70-74	«Удовлетворительно» (3)	удовлетворительно – неплохо, но со значительным количеством недостатков
60-69		удовлетворительно – выполнение удовлетворяет минимальные критерии
35-59	«Неудовлетворительно» (2)	неудовлетворительно – с возможностью повторной аттестации
0-34		неудовлетворительно – с обязательным повторным изучением дисциплины (выставляется комиссией)

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 стеганографической 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 (Инtranет)»

1. Идентификация и аутентификация.
2. Группы методов аутентификации.
3. Понятие учетной записи пользователя.
4. Особенности администрирования парольной системы, использующей многопарольные 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 (Инtranет)»

Организовать парольную защиту файлов средствами текстового редактора MS Word, электронной таблицы MS Excel, баз данных в MS Access.

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-пейджером, электронной почте, Интернет-сайтам и форумам, онлайн-играм);

В) адреса электронной почты других пользователей, IP-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 Windows в среде операционной системы MS-DOS.

5. Простейший макровирус в документе MicrosoftWord 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 Windows и (или) в инициализационном файле MicrosoftWord соответствующий флаг о произведенном заражении;

Г) при последующем запуске MicrosoftWord 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 MicrosoftWord.

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 неблагоприятных 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.