**Примерные оценочные материалы, применяемые при проведении**

**текущего контроля по дисциплине «Стандартизация и сертификация систем информационной безопасности»**

**ТЕСТИРОВАНИЕ ПО КУРСУ «СТАНДАРТИЗАЦИЯ И СЕРТИФИКАЦИЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ», тема «ГОСТы ИСО/МЭК 27000-27005»**

При проведении тестирования обучающемуся предлагается дать ответы на 35 вопросов из нижеприведенного списка. Тест считается сданным при не менее 30 правильных ответах.

1. Лицо или организационная единица, которое подтверждает, что разработанные структуры оценки защищенности подходят для оценки деятельности по обеспечению ИБ и результативности СМИБ, это:

- потребитель оценки защищенности

- рецензент оценки

- информационный аналитик

- планировщик оценки защищенности

1. Типы вспомогательных активов:

- бизнес-процессы;

- бизнес-приложения;

- информация;

- программно-технические средства;

1. Варианты обработки риска:

- анализ риска;

- оценка риска;

- снижение риска;

- предотвращение риска;

1. Руководство или другие заинтересованные стороны, запрашивающее или затребовавшее информацию об результативности СМИБ, это:

- потребитель оценки защищенности

- рецензент оценки

- информационный аналитик

- планировщик оценки защищенности

1. Попытка уничтожить, раскрыть, изменить, сделать недоступным, украсть или получить несанкционированный доступ или несанкционированно использовать актив это:

- атака

- угроза

- верификация

- инцидент ИБ

1. В рамках внутреннего аудита организация не должна:

- определить критерии и область аудита для каждой проверки;

- выбирать аудиторов и проводить аудиты так, чтобы гарантировать объективность и беспристрастность процесса аудита;

- сохранять документированную информацию как подтверждение программы аудита и его результатов;

- доводить результаты аудита до всех сотрудников службы ИБ.

1. Обеспечение гарантии того, что заявленные характеристики объекта являются подлинными это:

- сертификация

- аттестация

- аутентификация

- валидация

1. Политика в отношении мобильных устройств не должна предусматривать:

- регистрацию мобильных устройств;

- требования по электромагнитной защите;

- ограничения на установку программного обеспечения;

- требования к версиям программ и применяемым патчам.

1. Одно или несколько нежелательных или неожиданных событий ИБ, которые со значительной степенью вероятности подвергают опасности деловую деятельность и угрожают ИБ это:

- атака

- угроза

- верификация

- инцидент ИБ

1. При формировании плана резервного копирования должно быть учтено:

- при выполнении точных и полных записи резервных копий документирование процедур восстановления не требуется;

- объем (например, полное или частичное копирование) и частота резервного копирования выполняются одинаково для любой информации для обеспечения непрерывности деятельности организации;

- резервные копии должны храниться в удаленных местах, на существенном расстоянии для избежания повреждения в случае аварийных ситуаций в основном офисе;

- резервируемой информации должен быть обеспечен уровень защиты, как физической, так и от угроз внешнего воздействия, в соответствии с методическими указаниями ФСБ;

1. СМИБ включает следующие компоненты:

- документированная информация;

- политика;

- перечень технических средств;

- антивирусные базы данных;

1. Намерения и направление развития организации, официально сформулированные высшим руководством это:

- учредительный документ

- политика

- программа

- декларация

1. Скоординированные действия по руководству и управлению организацией в отношении рисков это:

- оценка риска

- анализ риска

- менеджмент риска

- определение степени риска

1. Возможная причина нежелательного инцидента, который может нанести ущерб системе или организации это:

- атака

- угроза

- верификация

- инцидент ИБ

1. Подтверждение получением объективных свидетельств, что требования для конкретного предполагаемого использования или применения были выполнены это:

- верификация

- валидация

- сертификация

- аттестация

1. СМИБ это

- система модернизации ИБ

- система менеджмента ИБ

- система малого инновационного бизнеса

- стандарт международной ИБ

1. Руководство устанавливает политику ИБ, которая:

- соответствует названию организации;

- включает цели (задачи) в области ИБ или служит основой для задания таких целей (задач);

- включает обязательство соответствовать действующим требованиям, связанным с ИБ;

- включает обязательство непрерывного улучшения системы менеджмента качества продукции.

1. Цели в области ИБ не должны быть:

- согласованными с политикой ИБ;

- измеримыми (если возможно);

- сообщены персоналу;

- утверждены в вышестоящей организации

1. Предварительная проверка персонала не должна включать:

- проверку физического здоровья кандидата,

- подтверждение заявленного образования и профессиональной квалификации,

- независимую проверку личности (паспорт или иной подобный документ),

- более детальную проверку, например, кредитной истории или наличие криминального прошлого.

1. Подтверждение получением объективных свидетельств, что заданные требования были выполнены это:

- верификация

- валидация

- сертификация

- унификация

1. Система управления паролями не должна:

- вынуждать использовать пароли надлежащего качества;

- принудительно заставлять пользователей менять пароли в ходе первой сессии;

- заставлять регулярно или по мере необходимости менять пароли;

- отображать (по требованию) вводимые пароли;

1. Требования к организации выноса активов не предусматривают:

- определение сотрудников, которые имеют право выдавать разрешения на вынос активов;

- установление сроков возврата актива и проверку их соблюдения;

- регистрацию выноса и возврата актива;

- регистрацию адреса, по которому осуществляется доставка активов.

1. Политика чистого стола и чистого экрана рекомендует:

- отпечатки, содержащие уязвимую или классифицированную информацию, необходимо забирать из печатающих устройств немедленно;

- регулярную уборку и обработку рабочих столов чистящими средствами;

- регулярную обработку мониторов ПК чистящими средствами;

- не должно допускаться несанкционированное использование копировальных аппаратов;

1. К внутренним заинтересованным сторонам СМИБ относятся:

- регуляторы и законодатели;

- специалисты по ИБ;

- клиенты и потребители;

- акционеры, включая собственников и инвесторов.

1. Решение не быть вовлеченным в рискованную ситуацию или действие, предупреждающее вовлечение в нее, это:

- идентификация риска;

- снижение риска;

- предотвращение риска:

- перенос риска;

1. Процесс нахождения, составления перечня и описания элементов риска, это:

- идентификация риска;

- снижение риска;

- предотвращение риска:

- перенос риска;

1. Процесс присвоения значений вероятности и последствий риска, это:

- коммуникация риска;

- снижение риска;

- предотвращение риска:

- количественная оценка риска;

1. Виды активов:

- дополнительные;

- основные;

- вспомогательные;

- производные;

1. Влияние неопределенности на цели это:

- вероятность

- риск

- атрибут

- угроза

1. Типы основных активов:

- бизнес-процессы;

- бизнес-приложения;

- информация;

- программно-технические средства;

1. Подтверждение соответствия третьей стороной, относящееся к продукции, процессам, системам или персоналу это:

- верификация

- валидация

- сертификация

- унификация

1. Действия по улучшению СМИБ не включают:

- анализ и оценку существующей ситуации для определения областей улучшения;

- формализованную фиксацию изменений;

- стандартизацию возможных решений

- поиск возможных решений для достижения этих целей;

1. Политика информационной безопасности должна быть:

- оформлена как справочная информация;

- доведена до сведения сотрудников в организации;

- доступной в установленном порядке для заинтересованных сторон

- утверждена в вышестоящей организации

1. Разделение среды разработки, тестирования и эксплуатации предусматривает:

- среда разработки и рабочая среда должны быть запущены в разных системах или на разных компьютерах и в разных доменах или директориях;

- изменения в рабочих системах и приложениях должны тестироваться в рабочей среде на рабочих системах;

- тестирования должны проводиться на рабочих системах, кроме как в случае возникновения исключений;

- компиляторы, редакторы и другой инструментарий для разработки или системные утилиты должны быть доступны из рабочих систем;

1. К внешним заинтересованным сторонам СМИБ относятся:

- регуляторы и законодатели;

- специалисты по ИБ;

- сотрудники отдела кадров;

- акционеры, включая собственников и инвесторов.