Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н., доцент И.Л. Рева
“___” _____г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ДИСЦИПЛИНЫ

Управление информационной безопасностью

Образовательная программа: 10.04.01 Информационная безопасность, магистерская программа: Методы и средства обеспечения технической защиты информации

Новосибирск 2023

1. Методика оценки этапов формирования компетенций по дисциплине

Уровни сформированности компетенций проверяется при проведении мероприятий текущей аттестации (контроля) в процессе изучения дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 3 семестре - в форме зачета, который направлен на оценку сформированности компетенций УК-2, ОПК-3, УК-3 и соотнесенных с ними индикаторов.

Зачет проводится в форме письменного тестирования с использованием электронной информационно-образовательной среда НГТУ (http:// www.nstu.ru/sveden/eos).

Общие правила выставления оценок текущей и промежуточной аттестации по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе дисциплины.

На основании приведенных далее критериев можно оценить уровни сформированности компетенций УК-2, ОПК-3, УК-3, закрепленных за дисциплиной.

2. Общая характеристика уровней освоения компетенций

Продвинутый. Теоретическое содержание курса освоено полностью. Студент демонстрирует систематическое и глубокое понимание учебного материала по системе обеспечения ИБ и способность к самостоятельному пополнению и обновлению знаний в ходе дальнейшей учебной работы и профессиональной деятельности. Сформированы необходимые навыки практической работы: расследование компьютерных инцидентов, внедрение СУИБ организации. Все учебные задания, предусмотренные программой обучения, выполнены качественно, без замечаний. Уровень сформированности компетенций и соотнесенных с ними индикаторов, закрепленных за дисциплиной, оценен числом баллов, входящим в диапазон продвинутого уровня.

Базовый. Теоретическое содержание курса освоено в объеме, необходимом для дальнейшей учебы и профессиональной деятельности. Навыки практической работы сформированы на базовом уровне: понимание расследования компьютерных инцидентов, этапов построения СУИБ организации. Все предусмотренные программой обучения учебные задания выполнены с небольшими погрешностями. Уровень сформированности компетенций и соотнесенных с ними индикаторов, закрепленных за дисциплиной, оценен числом баллов в пределах базового уровня.

Пороговый. Теоретическое содержание курса освоено, необходимом для дальнейшей учебы и профессиональной деятельности. Некоторые практические навыки работы с сформированы с незначительными пробелами. Учебные задания, предусмотренные программой обучения, выполнялись с ошибками, исправленными под руководством преподавателя. Недостаточный уровень теоретических знаний в области построения СУИБ организации. Уровень сформированности компетенций и соотнесенных с ними индикаторов, закрепленных за дисциплиной, оценен числом баллов в пределах порогового уровня.

Ниже порогового. Теоретическое содержание курса освоено фрагментарно. Необходимые навыки практической работы сформированы минимально. Большинство учебных заданий, предусмотренных программой обучения, не выполнены. Отсутствует комплексное понимание СУИБ организации, безопасности информационных потоков организации. Уровень сформированности компетенций и соотнесенных с ними индикаторов, закрепленных за дисциплиной, оценен числом баллов, входящих в диапазон ниже порогового уровня.

Паспорт зачета

по дисциплине «Управление информационной безопасностью», 3 семестр

1. **Методика оценки**

Зачет проводится в форме письменного тестирования с использованием электронной информационно-образовательной среда НГТУ (http:// www.nstu.ru/sveden/eos).

Тестовые задания охватывают все содержание «Управление информационной безопасностью» (модуля).

Тест состоит из вопросов различного вида и позволяет проверить результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций.

2. **Критерии оценки результатов обучения, соотнесенных с уровнями освоения индикаторов достижения компетенций**

Выполнение теста засчитывается на **продвинутом** уровне, если студент правильно ответил на все вопросы теста, знает определения всех понятий, продемонстрировал способность безошибочно устанавливать последовательность и соответствие между процессами и явлениями, выявлять проблемы, предлагать механизмы их решения, представляет количественные и качественные характеристики определенных процессов. Совокупность результатов обучения по дисциплине (модулю) и соотнесенных с ними индикаторов достижения компетенций не содержит пробелов. Установленные в программе компетенции сформированы в полном объеме. Оценка составляет *от 18 до 20 баллов.*

Выполнение теста засчитывается на **базовом** уровне, если студент правильно ответил на % вопросов теста, знает определения основных понятий, продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, правильно характеризует процессы, явления. Совокупность результатов обучения по дисциплине (модулю) и соотнесенных с ними индикаторов достижения компетенций содержит несущественные пробелы. Установленные в программе компетенции сформированы на базовом уровне. Оценка составляет *от 15 до 17 баллов.*

Выполнение теста засчитывается на **пороговом** уровне, если студент правильно ответил от V_2 до % вопросов теста, знает определения основных понятий, продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, допускает непринципиальные ошибки, например, вычислительные. Совокупность результатов обучения по дисциплине (модулю) и соотнесенных с ними индикаторов достижения компетенций содержит пробелы. Установленные в программе компетенции сформированы на пороговом уровне. Оценка составляет *от 10 до 14 баллов.*

Выполнение теста считается **неудовлетворительным**, если студент правильно ответил менее чем на половину вопросов теста, не знает определений понятий, не продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, допускает принципиальные ошибки. Совокупность результатов обучения по дисциплине (модулю) и соотнесенных с ними индикаторов достижения компетенций содержит существенные пробелы. Установленные в программе компетенции не сформированы. Оценка составляет *менее 10 баллов.*

3. **Шкала оценки**

Зачет считается сданным, если сумма баллов по всем заданиям составляет от 10 до 20 баллов включительно. Сумма менее 10 баллов признается неудовлетворительным результатом промежуточной аттестации по дисциплине.

В общей оценке по дисциплине баллы за зачет учитываются в соответствии с правилами балльно-рейтинговой системы, установленными в НГТУ.

4. Фонд оценочных материалов (вопросы теста) для оценки уровня сформированности компетенций и соотнесенных с ними индикаторов

Формируемая компетенции	Индикаторы компетенции
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	1. знает методы управления проектами; этапы жизненного цикла проекта 2. умеет разрабатывать и анализировать альтернативные варианты проектов для достижения намеченных результатов; разрабатывать проекты, определять целевые этапы и основные направления работ 3. владеет навыками: разработки проектов в избранной профессиональной сфере; методами оценки эффективности проекта, а также потребности в ресурсах

Вопросы теста для оценки сформированности компетенции УК-2

Вопрос 1. Какое обозначение имеет стандарт, содержащий свод норм и правил применения мер обеспечения информационной безопасности в организации?

- ГОСТ Р ИСО/МЭК 27000-2021
- ГОСТ Р ИСО/МЭК 27001-2021
- ГОСТ Р ИСО/МЭК 27002-2021 ✓
- ГОСТ Р ИСО 31000-2019

(один вариант)

Вопрос 2. Назовите основные вопросы, которые необходимо рассмотреть при разработке политики, определяющей условия и ограничения для дистанционной работы

Ответ:

Решение:
При разработке политики, определяющей условия и ограничения для дистанционной работы, следует рассмотреть следующие вопросы: a) существующая физическая защита удаленного места работы с учетом физической безопасности здания и местности; 5 b) предлагаемая физическая среда дистанционной работы; c) требования к безопасности связи с учетом необходимости удаленного доступа к внутренним системам организации, чувствительности этих систем, а также с учетом информации ограниченного доступа, к которой будут осуществлять доступ и которую будут передавать по линиям связи; d) предоставление доступа к виртуальному рабочему столу, который предотвращает обработку и хранение информации на личном оборудовании; e) угроза несанкционированного доступа к информации или ресурсам со стороны других лиц, находящихся в этом же помещении, например членов семьи или друзей; f) использование домашних сетей и установление требований или ограничений на конфигурацию сервисов беспроводных сетей; g) политики и процедуры для предотвращения споров, касающихся прав на интеллектуальную собственность, разработанную на личном оборудовании; h) доступ к личному оборудованию (для проверки его безопасности или в ходе расследования) может быть запрещен законодательством; i) лицензионные соглашения на программное обеспечение, в соответствии с которыми организация может нести ответственность за лицензирование клиентского программного обеспечения на личных рабочих станциях работников или внешних пользователей; j) требования к защите от вредоносных программ и межсетевым экранам.

Вопрос 3. Какие условия необходимо соблюсти при распределении ответственности по обеспечению информационной безопасности?

- для каждого актива или процесса ИБ следует назначить ответственное лицо, при этом следует детально задокументировать возложенную ответственность
- должны быть определены и задокументированы уровни полномочий
- чтобы иметь возможность выполнять возложенные обязанности, назначенные лица должны быть компетентны в области ИБ и им должна быть предоставлена возможность поддержания своих компетенций на должном уровне
- должны быть определены и задокументированы аспекты взаимодействия и контроля ИБ при взаимодействии с поставщиками
- все варианты верны ✓

(один вариант)

Вопрос 4. Что представляет собой риск информационной безопасности?

- комбинация вероятностей реализации угроз ИБ и наличия соответствующих уязвимостей

- комбинация последствий, вытекающих из нежелательного события информационной безопасности и
- вероятности возникновения события ✓
- вероятность возникновения нежелательного события ИБ
- количественная и качественная оценка последствий, вытекающих из реализации угроз ИБ
- комбинация стоимости информационных активов и вероятности возникновения нежелательного события в отношении данных активов

(один вариант)

Вопрос 5. Опишите действия при увольнении работника или расторжения договора с внешним пользователем в случаях, когда работник или внешний пользователь купил оборудование организации, или использует свое личное оборудование, или обладает знаниями, важными для деятельности организации.
Ответ:

Решение:
В тех случаях, когда работник или внешний пользователь купил оборудование организации или использует свое личное оборудование, необходимо соблюдать процедуры, обеспечивающие передачу всей соответствующей информации в организацию и ее безопасное удаление из оборудования.
В тех случаях, когда работник или внешний пользователь обладает знаниями, важными для текущей деятельности, такого рода информация должна быть задокументирована и передана в организацию.

Вопрос 6 Назовите вопросы, которые необходимо рассмотреть при установлении процедур по утилизации носителей информации.
Ответ:

Решение:
При установлении процедур по утилизации носителей информации необходимо рассмотреть следующие вопросы:
a) носители, содержащие конфиденциальную информацию, следует хранить и надежно утилизировать, например, посредством сжигания или измельчения, или же стирания информации, если носители планируют использовать для другого приложения в пределах организации; b) должны существовать процедуры по выявлению элементов, для которых может потребоваться надежная утилизация; c) может оказаться проще организовать сбор и надежную утилизацию в отношении всех носителей информации, чем пытаться выделить носители с информацией ограниченного доступа; d) многие организации предлагают услуги по сбору и утилизации носителей; следует уделять особое внимание выбору подходящего подрядчика с учетом имеющегося у него опыта и применяемых адекватных мер обеспечения безопасности; e) утилизацию носителей, содержащих информацию ограниченного доступа, следует фиксировать как контрольную запись для аудита.

Вопрос 7. Дайте описание руководства по применению меры информационной безопасности "Регистрация и отмена регистрации пользователей" класса "Процесс управления доступом пользователей".
Ответ:

Решение:
Процесс управления идентификаторами пользователей должен включать в себя:
a) использование уникальных идентификаторов пользователей, позволяющих отследить действия пользователей, чтобы они несли ответственность за свои действия; использование групповых идентификаторов должно быть разрешено только в тех случаях, когда это необходимо для бизнеса или в силу операционных причин и должно быть утверждено и документировано; b) немедленное отключение или удаление идентификаторов пользователей, покинувших организацию; c) периодическое выявление и удаление или отключение избыточных идентификаторов пользователей; d) обеспечение того, чтобы избыточные идентификаторы пользователей не были переданы другим пользователям

Вопрос 8. Приведите формулировку меры информационной безопасности "Аннулирование или корректировка прав доступа" класса "Процесс управления доступом пользователей".
Ответ:

Решение:
Права доступа всех работников и внешних пользователей к информации и средствам ее обработки должны быть аннулированы. После их увольнения, истечения срока действия договора или соглашения) либо скорректированы в случае необходимости

Вопрос 9. Что является нематериальной формой информации?
- знания
- концепции
- идеи
- бренды
- все варианты верны ✓

(один вариант)

Вопрос 10. Дайте описание руководства по применению меры информационной безопасности "Процесс управления секретной аутентификационной информацией пользователей" класса "Процесс управления доступом пользователей".
Ответ:

Решение:
Этот процесс контроля предоставления секретной аутентификационной информации должен включать в себя следующие требования:
a) пользователи должны подписывать соглашение о сохранении конфиденциальности личной секретной аутентификационной информации и секретной аутентификационной информации группы; b) в тех случаях, когда пользователи должны сами обеспечивать сохранность своей секретной аутентификационной информации, им вначале должна быть выдана временная секретная информация аутентификации, которую они должны изменить при первом использовании; c) должны быть установлены процедуры для проверки личности пользователя перед предоставлением новой (в том числе временной) секретной аутентификационной информации или заменой старой информации; d) временная секретная аутентификационная информация должна передаваться пользователю безопасным способом; следует избегать использования третьих сторон или незащищенного (открытого) текста сообщений электронной почты; e) временная секретная аутентификационная информация должна быть уникальной для конкретного пользователя и не должна быть легко угадываемой; f) пользователи должны подтвердить получение секретной аутентификационной информации; g) секретная аутентификационная информация, установленная по умолчанию производителем, должна быть изменена после установки системы или программного обеспечения.

Вопрос 11. В чем необходимо удостовериться при приеме работника для выполнения роли по информационной безопасности:
- кандидат обладает высокой физической выносливостью
- кандидат обладает знаниями в области информационной безопасности ✓
- кандидат имеет лидерские качества
- кандидат обладает навыками переговорщика
- кандидат имеет опыт работы в системе документооборота

(один вариант)

Вопрос 12. Опишите процедуры предоставления или аннулирования прав доступа к информации, средствам обработки информации.
Ответ:

Решение:
Предоставление или аннулирование прав доступа к информации или средствам обработки информации обычно представляет собой двухэтапную процедуру:
a) назначение и активация или аннулирование идентификатора пользователя; b) предоставление или аннулирование прав доступа для этого идентификатора пользователя.

Вопрос 13. К какому виду документа относится ГОСТ Р ИСО/МЭК 27002–2021 "Информационные технологии. Методы и средства обеспечения безопасности..."?

- справочно-информационному ✓
- нормативному
- организационно-правовому
- распорядительному
- научно-техническому

(один вариант)

Вопрос 14. Какое условие, учитывающееся при выборе меры обеспечения информационной безопасности, из ниже представленных является второстепенным
Требования государственных законодательных актов
Экономическая целесообразность
Возможное негативное влияние на бизнес-процессы
Техническая ресурсоемкость

Ответ:

Решение: Техническая ресурсоемкость

Вопрос 15. Какие области менеджмента информационной безопасности требуют проведения дополнительной оценки на наличие ресурсов перед запуском процесса менеджмента риска?

- мониторинг процесса менеджмента
- риска информационной безопасности
- выполнение оценки рисков и создания плана по обработке рисков
- пределение и реализация политик и процедур, включая реализацию выбранных мер и средств контроля и управления
- все варианты верны ✓

(один вариант)

Вопрос 16. Приведите формулировку меры информационной безопасности "Предоставление пользователю права доступа" класса "Процесс управления доступом пользователей".
Ответ:

Решение:
Должен быть реализован формализованный процесс назначения. Или отмены прав доступа пользователей к системам и сервисам.

Вопрос 17. Назовите основные требования к "Политике использования личных мобильных устройств в организации" класса "Мобильные устройства и дистанционная работа"

Ответ:

Решение:
Там, где допускается использование личных мобильных устройств, политика и соответствующие меры обеспечения информационной безопасности должны предусматривать: a) разделение использования устройств в личных и рабочих целях, включая использование программного обеспечения для обеспечения такого разделения и защиты информации ограниченного доступа на личном устройстве; b) предоставление доступа к информации ограниченного доступа только после того, как пользователи подпишут соглашение, признающее их обязанности (физическая защита, обновление программного обеспечения и т.д.), отказ от владения информацией ограниченного доступа, позволяющее организации дистанционно удалять данные в случае кражи или утери устройства, или когда пользователь больше не авторизован на использование. Политика должна учитывать особенности законодательства по защите конфиденциальной информации

Вопрос 18. Перечислите факторы, которые необходимо учитывать при разработке "Политики управления доступом".

Ответ:

Решение:
Политика управления доступом должна учитывать следующее:
a) требования безопасности бизнес-приложений; b) политики распространения информации и авторизации, уровни информационной безопасности и категорирование информации; c) соответствие между правами доступа и политиками категорирования информации для систем и сетей; d) соответствующие законодательные и любые договорные обязательства, касающиеся ограничения доступа к данным или сервисам; 15 e) управление правами доступа в распределенных средах и сетях, которые допускают все типы соединений; f) разделение ролей по управлению доступом, например запрос доступа, авторизация доступа, администрирование доступа; g) требования к формальной авторизации запросов доступа; h) требования к периодическому пересмотру прав доступа; i) аннулирование прав доступа; j) архивирование записей всех значимых событий, касающихся использования и управления идентификаторами пользователей и секретной аутентификационной информацией; k) роли с привилегированным доступом.

Вопрос 19. При каком условии применяются компенсирующие меры?
Ответ:

Решение:
Компенсирующие меры применяются в случае невозможности их реализации мерами, подлежащими реализации в соответствии с предъявляемыми к информационной (автоматизированной) системе требованиями по защите информации.

Вопрос 20. Соотнесите модели доступа с описанием
1) Дискреционная
2) Мандатная
3) Ролевая
4) Атрибутная

а) Доступ субъекту выдается на основе его должности или рабочего подразделения
б) Доступ к ресурсам предоставляется на основе правил, основывающихся на параметрах, присущих субъекту
в) Доступ предоставляется на основе уровня конфиденциальности, присвоенного каждому субъекту
г) Доступ основывается на списке субъектов, которым доступ может быть предоставлен, и списке объектов, к которым доступ может быть предоставлен.
Ответ:

Решение:
1) г
2) в
3) а
4) б

Вопрос 21. Приведите формулировку меры информационной безопасности "Информационная безопасность при управлении проектом" *Ответ:*

Решение:
Информационная безопасность должна рассматриваться при управлении проектом. Независимо от типа проекта

Вопрос 22. Дайте описание руководства по применению меры информационной безопасности "Пересмотр правдоступа пользователей" класса "Процесс управления доступом пользователей".
Ответ:

Решение:
При пересмотре прав доступа пользователей владельцы активов следует учитывать следующее:
a) права доступа пользователей следует пересматривать как через определенные интервалы времени, так и после любых изменений, таких как повышение или понижение в должности, или увольнение; b) права доступа пользователя следует пересматривать и переназначать в случае изменения его роли в организации; c) полномочия для привилегированных прав доступа следует пересматривать чаще; d) назначенные привилегии необходимо регулярно проверять для обеспечения уверенности в том, что никто не получил привилегий несанкционированным образом; e) изменения привилегированных учетных записей необходимо регистрировать для периодического анализа.

Вопрос 23. Дайте описание руководства по применению меры информационной безопасности "Доступ к сетям и сетевым сервисам" класса "Требование бизнеса по управлению доступом".

Ответ:

Решение:
В отношении использования сетей и сетевых сервисов должна быть сформулирована политика. Эта политика должна охватывать:
a) сети и сетевые сервисы, к которым разрешен доступ; b) процедуры авторизации для определения того, кому к каким сетям и сетевым сервисам разрешен доступ; c) меры управления и процедуры для защиты доступа к сетевым соединениям и сетевым сервисам; d) средства, используемые для доступа к сетям и сетевым сервисам (например, использование VPN или беспроводной сети); e) требования к аутентификации пользователя для доступа к различным сетевым сервисам; f) мониторинг использования сетевых сервисов.

Вопрос 24. Дайте описание руководства по применению меры информационной безопасности "Управление привилегированными правами доступа" класса "Процесс управления доступом пользователей".
Ответ:

Решение:
Назначение привилегированных прав доступа должно контролироваться посредством формализованного процесса аутентификации. В соответствии с действующей политикой управления доступом.

Вопрос 25. Дайте описание руководства по применению меры информационной безопасности "Информационная безопасность при управлении проектом"
Ответ:

Решение:
Информационная безопасность должна быть интегрирована в
метод(ы) управления проектами, чтобы гарантировать, что риски информационной безопасности идентифицированы и обработаны в рамках проекта. Применяемые методы управления проектами должны предусматривать следующее: a) цели информационной безопасности включены в цели проекта; b) оценку риска информационной безопасности проводят на ранней стадии проекта для определения необходимых вариантов его обработки; c) информационная безопасность является частью всех этапов применяемой методологии проекта.

Вопрос 26. Приведите формулировку меры информационной безопасности "Маркировка информации" класса

Решение:
Должен быть разработан и реализован соответствующий набор процедур маркировки информации в соответствии с принятой в организации системой категорирования информации.

Вопрос 27. Приведите формулировку меры информационной безопасности "Регистрация и отмена регистрации пользователей" класса "Процесс управления доступом пользователей".
Ответ:

Решение:
Для назначения прав доступа должна быть реализована формализованная процедура регистрации. И отмены регистрации пользователей.

Вопрос 28. Назовите требования, которые необходимо обеспечить при применении меры информационной безопасности "Управление привилегированными правами доступа" класса "Процесс управления доступом пользователей".
Ответ:

Решение:
При применении меры информационной безопасности "Управление привилегированными правами доступа" необходимо обеспечить следующие требования:
a) идентификация привилегированных прав доступа, связанных с каждой системой или процессом, например операционной системой, системой управления базами данных, каждым приложением и пользователями, которым требуется назначение таких прав; b) привилегированные права доступа должны назначаться пользователям исходя из принципов "необходимого использования" и "предоставления доступа по событию" в соответствии с политикой управления доступом, то есть по минимуму для их функциональных ролей; c) все процессы аутентификации и назначения привилегий должны регистрироваться. Привилегированные права доступа не должны предоставляться до завершения процесса аутентификации; d) должны быть определены требования для установления срока действия привилегированных прав доступа; e) привилегированные права доступа должны быть связаны с идентификатором пользователя, отличным от того, что используется для исполнения повседневных должностных обязанностей. Эти обязанности не должны выполняться под

привилегированным идентификатором; f) полномочия пользователей с привилегированными правами доступа должны регулярно пересматриваться с целью убедиться, что они соответствуют их обязанностям; g) должны быть разработаны и поддерживаться специальные процедуры, во избежание несанкционированного использования 19 общих административных идентификаторов в соответствии с возможностями конфигурации системы; h) при совместном использовании общих административных идентификаторов должна обеспечиваться конфиденциальность секретной аутентификационной информации. (например, частая смена паролей, а также максимально быстрая их смена при увольнении пользователя с привилегированными правами или изменении его обязанностей, передача паролей всем пользователям с привилегированными правами посредством соответствующих механизмов).

Вопрос 29. Приведите формулировку меры информационной безопасности "Допустимое использование активов" класса "Ответственность за активы"
Ответ:

Решение:
Должны быть идентифицированы. Документально оформлены и реализованы правила допустимого использования активов, включая информацию и средства ее обработки

Вопрос 30. Приведите формулировку меры информационной безопасности "Политика использования мобильных устройств" класса "Мобильные устройства и дистанционная работа".
Ответ:

Решение:
Должна быть определена политика. Реализованы поддерживающие
меры обеспечения информационной безопасности для управления рисками информационной безопасности, связанными с использованием мобильных устройств

Формируемая компетенции	Индикаторы компетенции
ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	1. умеет разрабатывать организационно-распорядительную документацию по обеспечению информационной безопасности 2. владеет навыками расчета и управления рисками информационной безопасности 3. знает основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью

Вопросы теста для оценки сформированности компетенции ОПК-3

Вопрос 1. Какие категории сотрудников организации обеспечивают внедрение эффективной системы менеджмента информационной безопасности?

- **все сотрудники организации ✓**
- только специалисты по ИБ
- только специалисты по ИТ
- только руководство

(один вариант)

Вопрос 2. Какие критерии могут учитываться при установлении категорирования информации по конфиденциальности:

- раскрытие информации не приведет к ущербу
- раскрытие информации приведет к незначительным затруднениям или незначительным неудобствам в операционной деятельности
- раскрытие информации оказывает значительное кратковременное влияние на операционную деятельность или достижение тактических целей
- раскрытие информации оказывает серьезное влияние на достижение долгосрочных стратегических целей
- или подвергает риску само существование организации
- **все варианты верны ✓**

(один вариант)

Вопрос 3. Какой актив представляют ценность для деятельности организации и нуждается в защите от различных угроз информационной безопасности?

- процессы
- системы
- сети
- информация
- **все варианты верны ✓**

(один вариант)

Вопрос 4. Как именуется метка, предназначенная для маркировки конфиденциальной информации?

- штамп
- хэш-сумма
- **гриф секретности ✓**
- отпечаток
- ЭП

(один вариант)

Вопрос 5. Основная причина низкой эффективности системы информационной безопасности в организациях?

- недостаток поддержки со стороны руководства организации
- политика безопасности не отвечает реальным угрозам
- недостаточная квалификации сотрудников по информационной безопасности
- ограничение бюджета на информационную безопасность
- **все варианты верны ✓**

(один вариант)

Вопрос 6. Дополните. При использовании мобильных устройств особое внимание следует уделять тому, чтобы информация _____ _____ не была скомпрометирована. Политика использования мобильных устройств должна принимать во внимание риски работы с мобильными

устройствами в незащищенных средах
Ответ:

Решение:
Ограниченного доступа

Вопрос 7. Какие ограничения влияют на организацию и определяют направленность ее информационной безопасности?

- ограничения политического свойства
- ограничения, на возникновение которых влияет состояние экономики и политики
- структурные ограничения
- функциональные ограничения
- **все варианты верны ✓**

(один вариант)

Вопрос 8. Дополните. Владельцы активов должны определить соответствующие правила управления доступом. Права доступа и ограничения для конкретных пользовательских ролей по отношению к своим активам с уровнем детализации и строгостью мер, отражающих _____, связанные с обеспечением информационной безопасности

Ответ:

Решение:
риски

Вопрос 9. Дополните. Меры информационной безопасности "Процесс управления секретной аутентификационной информацией пользователей" звучат следующим образом: предоставление секретной аутентификационной информации должно контролироваться посредством Предоставление формального

_____ _____.
Ответ:

Решение:
процесса управления

Вопрос 10. Назовите 4 уровня политики ИБ.

- Общая политика
- Частные политики
- Процедуры и инструкции
- Документирование
- **Все варианты верны ✓**

(один вариант)

Вопрос 11. Назовите основное требование к "Политике использования мобильных устройств"
Ответ:

Решение:
регистрация мобильных устройств

Вопрос 12. Что такое "эффект накопления", учитываемый при утилизации носителей информации?

- большое количество носителей информации трудно утилизировать
- **большое количество информации неограниченного доступа, хранящейся на утилизируемых носителях, в совокупности может представлять собой конфиденциальную информацию ✓**
- электромагнитные носители информации после размагничивания могут содержать остаточные следы данных
- большие трудозатраты на оформление актов утилизации

(один вариант)

Вопрос 13. Приведите формулировку меры информационной безопасности "Пересмотр прав доступа пользователей".
Ответ:

Решение:
Права доступа должны пересматриваться

Вопрос 14. Дайте описание жизненного цикла информации

- Хранение, обработка, использование, передача
- Хранение, использование
- Хранение, обработка
- Создание, уничтожение
- **Создание, хранение, обработка, использование, передача, уничтожение ✓**

(один вариант)

Вопрос 15. Дайте определение принципу минимальных привилегий.

- минимум прав доступа и их расширение из расчета стажа работы
- перманентный доступ ко всей информации
- **доступ только к такой информации и ресурсам, которые минимально необходимы для успешного выполнения его рабочих задач ✓**

(один вариант)

Вопрос 16. Приведите формулировку меры информационной безопасности "Дистанционная работа"
Ответ:

Решение:
Организация защиты удаленных подключений

Вопрос 17. Приведите формулировку меры информационной безопасности "Политика управления доступом".
Ответ:

Решение:
Политика должна пересматриваться

Вопрос 18. Приведите формулировку меры информационной безопасности "Перемещение физических носителей".
Ответ:

Решение:
Защита физических носителей

Вопрос 19. Назовите факторы, определяющие порядок аннулирования или корректировки прав доступа работников, контрагентов.
- кем было инициировано прекращение или изменение трудовых отношений: работником, сторонним пользователем или руководством, а также причина прекращения отношений
- текущие обязанности работника, внешнего пользователя или любого другого пользователя
- ценность активов, находящихся в текущем доступе
- **все перечисленное ✓**

(один вариант)

Вопрос 20. Дайте описание руководства по применению меры информационной безопасности "Перемещение физических носителей" класса "Обращение с носителями информации".
- должен использоваться надежный транспорт или курьеры
- перечень авторизованных курьеров должен быть согласован с руководством
- должны быть разработаны процедуры для идентификации курьеров
- упаковка должна обеспечивать защиту содержимого от любых физических повреждений, которые могут возникнуть в ходе транспортировки, и соответствовать требованиям производителей
- должны регистрироваться записи о содержании носителей, применяемых мерах обеспечения ИБ, а также о времени передачи курьеру для транспортировки и времени получения в пункте назначения
- **все перечисленное ✓**

(один вариант)

Вопрос 21. В организациях, предусматривающих возможность дистанционной работы, должна издаваться политика, определяющая условия и ограничения для дистанционной работы. Как называется данная политика?
Ответ:

Решение:
Дистанционная работа

Вопрос 22. Назовите набор мер, необходимых для обеспечения информационной безопасности организации
Ответ:

Решение:
Организационные и технические

Вопрос 23. Приведите формулировку меры информационной безопасности "Возврат активов"
Ответ:

Решение:
пользователи должны возвращать активы

Вопрос 24. Приведите формулировку меры информационной безопасности "Инвентаризация активов"
Ответ:

Решение:
активы надо идентифицировать

Вопрос 25. Дайте описание руководства по применению меры информационной безопасности "Утилизация носителей информации".
Ответ:

Решение:
Носители информации надо уничтожать

Вопрос 26. Дополните. Организация должна идентифицировать активы, относящиеся к жизненному циклу информации, и задокументировать их значимость. Жизненный цикл информации должен включать в себя создание, обработку, хранение, _____, удаление и уничтожение. Документация должна храниться в специально созданных или уже существующих перечнях, в зависимости от ситуации

Ответ:

Решение:
передачу

Вопрос 27. Дополните. Необходимо, чтобы процедуры маркировки информации охватывали информационные активы, представленные как в физической, так и в _____ форме. Маркировка должна соответствовать системе категорирования. Маркировка должна легко распознаваться. Процедуры должны содержать указания относительно того, где и как размещается маркировка, с учетом того, каким образом осуществляется доступ к информации или каким образом обрабатываются активы, в зависимости от типов носителей.

Ответ:

Решение:
электронной

Вопрос 28. Приведите формулировку меры информационной безопасности "Утилизация носителей информации"
Ответ:

Решение:
Носители информации необходимо утилизировать

Вопрос 29. Назовите требования к перечню активов в рамках применения меры информационной безопасности "Инвентаризация активов"
Ответ:

Решение:
Перечень должен быть актуальным

Вопрос 30. Назовите категорию мер информационной безопасности, целью которой является обеспечить уверенность в том, что в отношении информации обеспечивается надлежащий уровень защиты в соответствии с ее значимостью для организации.

Ответ:

Решение:
Категорирование информации

Формируемая компетенции	Индикаторы компетенции
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	1. знает методики формирования команд; методы эффективного руководства коллективами 2. умеет разрабатывать командную стратегию; организовывать работу коллективов; управлять коллективом; разрабатывать мероприятия по личностному, образовательному и профессиональному росту 3. владеет методами организации и управления коллективом, планированием его действий

Вопросы теста для оценки сформированности компетенции УК-3

Вопрос 1. Какие требования по информационной безопасности необходимо обеспечить при перемещении физических носителей, содержащих информацию?

- необходимо перемещать носители исключительно с привлечением физически сильных уполномоченных лиц
- необходимо перемещать носители исключительно в дневное время
- перемещаемые носители необходимо защитить от несанкционированного доступа, ненадлежащего использования или повреждения ✓
- перемещаемые носители необходимо оснастить световыми сигналами
- необходимо упаковать перемещаемый носитель в упаковку определенного цвета

(один вариант)

Вопрос 2. Что понимается под территориальными ограничениями, влияющими на организацию и определяющими направленность ее информационной безопасности?

- климат, природные риски
- локализация рабочих площадок и инфраструктуры организации ✓
- функциональная структура организации
- законодательные и нормативные акты
- наличие у организации прав собственности

(один вариант)

Вопрос 3. Что понимается под техническими ограничениями, влияющими на организацию и определяющими направленность ее информационной безопасности?

- регламенты, определяющие правила обработки информации
- требования, касающиеся длительности производственного цикла
- требования, касающиеся инструментальных средств разработки ПО
- требования, касающиеся уровня оценки, качества программного обеспечения ✓
- требования к режиму рабочего времени организации

(один вариант)

Вопрос 4. Какие меры необходимо применять при организации системы управления доступом?

- только организационные
- только логические
- только физические
- логические, физические и организационные совместно ✓
- нет правильного ответа

(один вариант)

Вопрос 5. Приведите формулировку меры информационной безопасности "Владение активами" класса "Ответственность за активы"
Ответ:

Решение:
Для каждого актива, включенного в перечень инвентаризации. Должен быть определен его владелец

Вопрос 6. Дайте описание руководства по применению меры информационной безопасности "Владение активами" класса "Ответственность за активы"
Ответ:

Решение:
Отдельные физические лица, так же как и юридические лица, имеющие утвержденную руководством ответственность за актив в течение его жизненного цикла, могут быть назначены в качестве владельцев активов. Владелец должен быть назначен при создании активов или при передаче активов в организацию. Владелец актива несет ответственность за выполнение требований информационной безопасности для данного актива.

Вопрос 7. Приведите формулировку меры информационной безопасности "Использование секретной аутентификационной информации" класса "Ответственность пользователей".
Ответ:

Решение:
При использовании секретной аутентификационной информации. Пользователи должны выполнять установленные в организации правила.

Вопрос 8. Назовите обязательства владельца актива в рамках применения меры информационной безопасности "Владение активами" класса "Ответственность за активы"
Ответ:

Решение:
Владелец актива должен:
a) обеспечить проведение инвентаризации активов; b) обеспечить, чтобы активы были должным образом категорированы и защищены; c) определять и периодически пересматривать ограничения доступа и категорирование важных активов с учетом действующих политик управления доступом; d) обеспечить надлежащие действия с активом, когда он удаляется или уничтожается.

Вопрос 9. Приведите формулировку меры информационной безопасности "Категорирование информации" класса "Ответственность за активы".
Ответ:

Решение:
Информация должна быть категорирована с точки зрения нормативных правовых требований, ценности, критичности. А также чувствительности к неавторизованному раскрытию или модификации.

Вопрос 10. Дайте описание руководства по применению меры информационной безопасности "Использование секретной аутентификационной информации" класса "Ответственность пользователей".
Ответ:

Решение:
При использовании секретной аутентификационной информации всем пользователям должно быть рекомендовано:
a) хранить секретную аутентификационную информацию в тайне, гарантируя, что она не будет разглашена никакой другой стороне, в том числе представителям органов власти; b) избегать хранения записей секретной аутентификационной информации (например, на бумаге, в файле программного обеспечения или на мобильном устройстве), кроме тех случаев, когда эти записи могут быть надежно сохранены, а способ хранения одобрен (например, хранилище паролей); c) изменять секретную аутентификационную информацию всякий раз, когда есть какие-либо признаки ее возможной компрометации; d) когда в качестве секретной аутентификационной информации используются пароли, необходимо выбирать стойкие пароли с достаточной минимальной длиной; e) не используют одну и ту же секретную аутентификационную информацию для деловых и частных целей.

Вопрос 11. Дайте описание руководства по применению меры информационной безопасности "Категорирование информации" класса "Ответственность за активы".
Ответ:

Решение:
Категорирование информации и связанные с ней меры обеспечения информационной безопасности должны учитывать потребности бизнеса в обмене информацией или ограничении доступа к ней, а также требования законодательства. Прочие активы, не являющиеся информацией, также могут быть категорированы в соответствии с категорированием информации, которая в них хранится, обрабатывается или иным образом преобразуется, или защищается этими активами. Владельцы информационных активов должны быть

ответственными за их категорирование.
Категорирование должно быть включено в процессы организации, быть согласованным и единообразным по всей организации. Результаты категорирования должны отражать ценность активов в зависимости от их чувствительности и критичности для организации, например, с точки зрения конфиденциальности, целостности и доступности.

Вопрос 12. Назовите рекомендации к выбору паролей, как вида секретной аутентификационной информации класса "Ответственность пользователей".
Ответ:

Решение:
Когда в качестве секретной аутентификационной информации используются пароли, необходимо выбирать стойкие пароли с достаточной минимальной длиной, которые:
1) легко запомнить; 2) не основаны на том, о чем кто-либо другой может легко догадаться или вычислить на основе личной информации, например имена, номера телефонов и даты рождения и т.д.; 3) неуязвимы к атакам по словарю (т.е. не состоят из слов, включенных в словари); 4) не содержат последовательности идентичных символов, не являются полностью цифровыми или буквенными; 5) если являются временными, изменяются при первом входе в систему; 6) не делятся секретной аутентификационной информацией; 7) помогают обеспечить надлежащую защиту в тех случаях, когда пароли используются в качестве секретной аутентификационной информации в процедурах автоматического входа и хранятся в системе.

Вопрос 13. Опишите систему категорирования активов в рамках применения меры информационной безопасности "Категорирование информации" класса "Ответственность за активы"
Ответ:

Решение:
Система категорирования должна включать в себя метки категорирования и критерии для пересмотра категорирования по истечении времени. Уровень защиты в системе должен оцениваться путем анализа конфиденциальности, целостности и доступности и любых других требований к рассматриваемой информации. Система должна быть согласована с политикой управления доступом.
Каждому уровню должно быть присвоено наименование, которое имеет смысл в контексте применения этой системы категорирования. Система должна быть единой для всей организации, чтобы лица, проводящие категорирование информации и связанных с ней активов, выполняли это одинаково, имели общее понимание требований по защите и применяли соответствующие меры по защите.

Вопрос 14. Приведите формулировку меры информационной безопасности "Ограничение доступа к информации" класса "Управление доступом к системам и приложениям".
Ответ:

Решение:
Доступ к информации должен быть ограничен. Доступ к функциям прикладных систем должен быть ограничен в соответствии с политикойуправления доступом.

Вопрос 15. Дайте описание руководства по применению меры информационной безопасности "Управление съемными носителями информации" класса "Обращение с носителями информации".
Ответ:

Решение:
Для управления съемными носителями необходимо рассмотреть и учесть следующие рекомендации: a) содержимое, в котором отпала необходимость, на любых перезаписываемых носителях, которые могут быть вынесены из организации, должно быть удалено без возможности восстановления; b) где это необходимо и целесообразно, должно требоваться разрешение на вынос носителей информации из организации, а записи о выносе следует хранить как контрольную запись для аудита; c) все носители следует хранить в безопасном, надежном месте в соответствии с инструкциями производителей; 12 d) если конфиденциальность или целостность данных являются важными факторами, следует использовать криптографические методы для защиты данных на съемных носителях; e) для снижения риска деградации носителей, когда сохраняемые данные все еще необходимы, данные должны быть перенесены на новые носители, прежде чем прежние станут нечитаемыми; f) несколько копий ценных данных следует хранить на отдельных носителях для снижения риска случайного повреждения или потери данных; g) для уменьшения возможности потери данных должна быть предусмотрена регистрация съемных носителей информации; h) съемные диски разрешается использовать только в случаях, обусловленных потребностями бизнеса; i) в случае необходимости использования съемных носителей перенос информации на них необходимо контролировать.

Вопрос 16. Дайте описание руководства по применению меры информационной безопасности "Ограничение доступа к информации" класса "Управление доступом к системам и приложениям".

Ответ:

Решение:
Ограничения доступа должны основываться на требованиях конкретных бизнес-приложений. Соответствовать установленной политике управления доступом.

Вопрос 17. Дайте описание руководства по применению меры информационной безопасности "Аннулирование или корректировка прав доступа" класса "Процесс управления доступом пользователей".
Ответ:

Решение:
После завершения трудовых отношений права доступа пользователя к информации и активам, связанным со средствами обработки информации и сервисов, должны быть удалены или приостановлены. Изменения в должности должны находить отражение в удалении всех прав доступа, которые не были одобрены для новой позиции. Права доступа, которые должны быть удалены или изменены, распространяются также на физический и логический доступ. Удаление или изменение прав доступа могут быть выполнены путем удаления, отзыва или замены ключей, идентификационных карточек, средств обработки информации или абонементов. Если работнику или внешнему пользователю, прекращающему работу известны пароли для остающихся активными логинов пользователей, они должны быть изменены после прекращения или изменения трудовых отношений, контракта или соглашения

Вопрос 18. Перечислите факторы, которые необходимо учитывать разработке требований по ограничению доступа к информации.

Ответ:

Решение:
Для обеспечения выполнения требований по ограничению доступа следует учитывать следующее: a) предоставление меню для управления доступом к функциям прикладных систем; b) управление тем, какие данные могут быть доступны конкретному пользователю; c) управление правами доступа пользователей, например чтение, запись, удаление и выполнение; d) управление правами доступа других приложений; e) ограничение информации, содержащейся в выходных данных; f) обеспечение физических или логических мер управления доступом для изоляции чувствительных приложений, данных или систем.

Вопрос 19. Приведите формулировку меры информационной безопасности "Управление съемными носителями информации" класса "Обращение с носителями информации".
Ответ:

Решение:
Должны быть реализованы процедуры по управлению сменными носителями информации. В соответствии с принятой в организации системой категорирования информации.

Вопрос 20. Дайте описание руководства по применению меры информационной безопасности "Возврат активов" класса "Ответственность за активы"
Ответ:

Решение:
Процесс прекращения трудовых отношений должен быть оформлен
таким образом, чтобы включать возврат всех ранее выданных физических и электронных активов, принадлежащих или доверенных организации. В течение некоторого периода времени после уведомления о прекращении трудовых отношений организация должна контролировать неавторизованное копирование соответствующей информации (например, интеллектуальной собственности) увольняемыми работниками и подрядчиками

Вопрос 21. Назовите вопросы, требуемые к рассмотрению при разработке процедуры для обращения, обработки, хранения и передачи информации в соответствии с ее категорированием.
Ответ:

Решение:
При разработке процедуры для обращения, обработки, хранения и передачи информации в соответствии с ее категорированием необходимо рассмотреть следующие вопросы:
a) ограничение доступа, обеспечивающее выполнение требований по защите для каждой категории; b) ведение официального учета уполномоченных обладателей активов; c) защита временных или постоянных копий информации на уровне, соответствующем уровню защиты оригиналов информации; d) хранение активов

информационных технологий в соответствии с инструкциями производителей; е) четкая маркировка всех копий носителей для информирования уполномоченного обладателя.

Вопрос 22. Приведите формулировку меры информационной безопасности "Безопасные процедуры входа в систему" класса "Управление доступом к системам и приложениям".
Ответ:

Решение:
Когда этого требует политика управления доступом. Доступ к системам и приложениям должен управляться посредством безопасной процедуры входа в систему.

Вопрос 23. Дайте описание руководства по применению меры информационной безопасности "Обращение с активами" класса "Ответственность за активы".
Ответ:

Решение:
Должны быть разработаны процедуры для обращения. Обработки, хранения и передачи информации в соответствии с ее категорированием.

Вопрос 24. Дайте описание руководства по применению меры информационной безопасности "Безопасные процедуры входа в систему" класса "Управление доступом к системам и приложениям".
Ответ:

Решение:
Должны быть выбраны подходящие методы аутентификации для подтверждения заявленной личности пользователя.
Там, где требуется строгая аутентификация и проверка личности, должны использоваться методы аутентификации, альтернативные паролям, такие как криптографические средства, смарт-карты, токены или биометрические средства. Процедура входа в систему или приложение должна быть разработана таким образом, чтобы минимизировать возможность несанкционированного доступа. Таким образом, процедура входа в систему должна раскрывать минимум информации о системе или приложении, во избежание оказания какой-либо неумышленной помощи неавторизованному пользователю.

Вопрос 25. Приведите формулировку меры информационной безопасности "Обращение с активами" класса "Ответственность за активы".
Ответ:

Решение:
Должны быть разработаны. Реализованы процедуры обращения с активами в соответствии с принятой в организации системой категорирования информации.

Вопрос 26. Дайте описание руководства по применению меры информационной безопасности "Допустимое использование активов" класса "Ответственность за активы"
Ответ:

Решение:
Работники и внешние пользователи, использующие или имеющие
доступ к активам организации, должны быть осведомлены о требованиях информационной безопасности, относящихся к информации, активам организации, связанным с информацией, средствам и ресурсам обработки информации. Они должны нести ответственность за использование ими любых ресурсов обработки информации и любое подобное использование, осуществляемое в зоне их ответственности

Вопрос 27. Что означает принцип "необходимого знания" при определении политики управления доступом:

- доступ предоставляется сотруднику только к тем средствам обработки информации, которые необходимы для выполнения работы
- при приеме сотрудников на работу, они проверяются на соответствие специальным проверочным стандартам
- сотрудник должен соответствовать критериям квалификационных и личностных характеристик
- доступ предоставляется сотруднику только к той информации, которая необходима ему для выполнения должностных обязанностей ✓
- озабоченность организации по поводу отношения служащих к своим обязанностям и возможных проблем,

(один вариант)

Вопрос 28. Какая из областей Политик информационной безопасности ориентирована на конечного пользователя?

- допустимое использование активов
- "чистый стол" и "чистый экран"
- передача информации
- ограничения на установку и использование программного обеспечения
- все варианты верны ✓

(один вариант)

Вопрос 29
Какое из утверждений о применимости мер обеспечения информационной безопасности, приведенных в стандарте ГОСТ Р ИСО/МЭК 27002–2021 "Информационные технологии. Методы и средства обеспечения безопасности...", является верным в отношении конкретной организации?

- применимы все меры и рекомендации, приведенные в стандарте
- применимы не все меры и рекомендации, приведенные в стандарте ✓
- применимы только технические меры и рекомендации
- применимы только организационные меры и рекомендации
- применимы только дополнительные меры и рекомендации

(один вариант)

Вопрос 30. Назовите цель применения категории мер информационной безопасности класса "Ответственность пользователей"
Ответ:

Решение:
Установить ответственность пользователей за защиту. Защиту их аутентификационной информации