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

Технологии защиты информации от несанкционированного доступа
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 1 семестре - в форме экзамена, который направлен на оценку сформированности компетенций ПК-1. В/ПР, ПК-5.В/ПР и соотнесенных с ними индикаторов.

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 ПК-1.В/ПР, ПК-5.В/ПР, закрепленных за дисциплиной.

2. Общая характеристика уровней освоения компетенций

Продвинутый. Теоретическое содержание курса освоено полностью. Студент демонстрирует систематическое и глубокое понимание учебного материала и способность к самостоятельному пополнению и обновлению знаний в ходе дальнейшей учебной работы и профессиональной деятельности. Сформированы необходимые навыки практической работы. 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. 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. 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. Уровень сформированности компетенций и соотнесенных с ними индикаторов, закрепленных за дисциплиной, оценен числом баллов, входящих в диапазон ниже порогового уровня.

Паспорт экзамена

по дисциплине «Технологии защиты информации от несанкционированного доступа», 1семестр

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 «Технологии защиты информации от несанкционированного доступа» (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 35 до 40 баллов.*

Выполнение теста засчитывается на **базовом** уровне, если студент правильно ответил на ⅔ 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 30 до 34 баллов.*

Выполнение теста засчитывается на **пороговом** уровне, если студент правильно ответил от ½ до ⅔ 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 20 до 29 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 20 баллов.*

3. Шкала оценки Зачет считается сданным, если сумма баллов по всем заданиям составляет от 20 до 40 баллов включительно. Сумма менее 20 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

ПК-1.В/ПР Способен применять решениядля организации систем защиты информации	1. знает требования по информационной безопасности для различных систем 2. умеет анализировать и оценивать угрозы информационной системы организации 3. знает требования нормативно-методических документов по организации систем защиты информации 4. умеет интегрировать системы защиты информации

Вопросы теста для оценки сформированности компетенции ПК-1.В/ПР

Вопрос 1. Угроза безопасности информации (компьютерной системы) —

- **потенциально возможное воздействие на информацию (компьютерную систему), которое прямо или косвенно может нанести урон пользователям или владельцам информации (компьютерной системы). ✔**
- субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации.
- свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).
- свойство компьютерной системы (среды, средств и технологии обработки), в которой циркулирует информация.

(один вариант)

Вопрос 2. Цель внешнего нарушителя безопасности информации —
Ответ:

Решение:
Преодоление периметра защиты

Вопрос 3. Какие механизмы должны использоваться в информационной системе для поддержки управления учетными записями пользователей, которые позволяют однозначно определить пользователя системы и проверить подлинность заявленной идентичности?
Ответ:

Решение:
Идентификации и аутентификации.

Вопрос 4. Конфиденциальность информации -

- **субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации. ✓**
- потенциально возможное воздействие на информацию, которое прямо или косвенно может нанести урон пользователям или владельцам информации.
- свойство информации, заключающееся в ее существовании в неискаженном виде.
- нарушение установленных ограничений на доступ к информации.

(один вариант)

Вопрос 5. Перечислите 3 основных принципа защиты информации.
Ответ:

Решение:
Конфиденциальность, целостность, доступность

Вопрос 6. В информационной системе должно осуществляться автоматическое блокирование временных учетных записей пользователей по окончании

Ответ:

Решение:

Установленного периода времени.

Вопрос 7. Целостность информации –

- **свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). ✓**
- потенциально возможное воздействие на информацию, которое прямо или косвенно может нанести урон пользователям или владельцам информации.
- нарушение установленных ограничений на доступ к информации.

(один вариант)

Вопрос 8. Что из перечисленного является основным принципом модели дискреционного разграничения доступа?

- **субъекту, которому были присвоены привилегии доступа к ресурсу, по своему усмотрению делегировать привилегии другим субъектам или группам субъектов. ✓**
- доступ к ресурсам контролируется с помощью ролей, предоставляемых пользователям.
- все доступы к ресурсам регулируются централизованно административной системой.
- права на доступ к ресурсам автоматически наследуются пользователями в пределах одного органа.

(один вариант)

Вопрос 9. Доступность информации –

свойство компьютерной системы (среды, средств и технологии обработки), в которой циркулирует
информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость. ✔

потенциально возможное воздействие на информацию (компьютерную систему), которое прямо или косвенно может нанести урон пользователям или владельцам информации (компьютерной системы).

субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации.

свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

(один вариант)

Вопрос 10. Что из перечисленного является характерной чертой мандатного разграничения доступа?

- **доступ к ресурсам контролируется центрально установленными правилами, которые не могут быть изменены пользователями. ✔**
- доступ к ресурсам предоставляется на основе индивидуальных пользовательских прав и профилей.
- правила доступа определяются на основе классификации информации и присвоенных пользователям ролей.
- пользователи могут на свое усмотрение менять правила доступа к информации, которой они владеют.

(один вариант)

Вопрос 11. В информационной системе должно осуществляться автоматическое блокирование учетных записей пользователей:

- если работник ушёл в отпуск
- **при выявлении по результатам мониторинга (просмотра, анализа) журналов регистрации событий безопасности действий пользователей, которые отнесены оператором к событиям нарушения безопасности информации ✔**
- учётные записи пользователей могут быть заблокированы только по истечении срока их действия
- учётные записи блокируются автоматически каждые 30 дней для проверки безопасности.

(один вариант)

12. Угроза конфиденциальности информации –

- **нарушение установленных ограничений на доступ к информации. ✓**
- несанкционированное изменение информации.
- несанкционированно блокируется доступ к информации
- преодоление защиты компьютерной системы.

(один вариант)

Вопрос 13. Угроза целостности информации –

- **несанкционированное изменение информации, случайное или преднамеренное. ✓**
- несанкционированно блокируется доступ к информации.
- нарушение установленных ограничений на доступ к информации.
- преодоление защиты компьютерной системы.

(один вариант)

Вопрос 14. Мандатное разграничение доступа. Разграничительное свойство безопасности

- **владельцы индивидуальных ресурсов могут назначать меры защиты объектов, которые они контролируют. ✓**
- пользователи могут устанавливать правила доступа к объектам на основе своих личных предпочтений.
- доступ к ресурсам системы регулируется на основе бизнес-ролей пользователей.
- права доступа предоставляются автоматически после прохождения процесса аутентификации.

(один вариант)

Вопрос 15. В информационной системе для заведения, активации, блокирования и уничтожения учетных записей пользователей и оповещение администраторов о результатах должен осуществляться *Ответ:*

Решение:
Автоматический контроль

Вопрос 16. Угроза доступности информации

- **осуществляется, когда несанкционированно блокируется доступ к информации (блокирование может быть постоянным или на некоторое время, достаточное, чтобы информация стала бесполезной). ✓**
- преодоление защиты компьютерной системы, выявление параметров, функций и свойств ее системы безопасности.
- нарушение установленных ограничений на доступ к информации.
- несанкционированное изменение информации, случайное или преднамеренное.

(один вариант)

Вопрос 17. Мандатное разграничение доступа. Простое свойство безопасности

- **субъекты с данным уровнем безопасности не могут читать данные, уровень секретности которых выше их собственного. ✓**
- пользователи имеют право изменять уровень секретности объектов в соответствии с их уровнем доступа.
- субъекты могут читать и писать данные на любом уровне секретности.
- доступ к данным предоставляется на основе выполненных операций пользователя.

(один вариант)

Вопрос 18. В информационной системе для управления доступом субъектов доступа к объектам доступа должны быть реализованы установленные оператором *Ответ:*

Решение:
Методы управления доступом.

Вопрос 19. Что из перечисленного является ключевым принципом модели разграничения доступа на основе ролей?

- **права доступа назначаются пользователям на основе их ролей в организации. ✓**
- права доступа назначаются исключительно администратором.
- права доступа автоматически одинаковы для всех пользователей.

(один вариант)

Вопрос 20. Какое утверждение лучше всего описывает модель разграничения доступа на основе идентификационных данных?

- **модель основана на присвоении доступа пользователям с уникальными идентификаторами, которые проверяются системой для авторизации доступа к ресурсам ✓**
- модель основана на предоставлении доступа на основе ip-адреса пользователя.
- модель использует физические ключи для разграничения доступа.

(один вариант)

Вопрос 21. Методы управления доступом реализуются в зависимости от особенностей функционирования _____ _____, с учетом угроз безопасности информации
Ответ:

Решение:
информационной системы

Вопрос 22. Какой из следующих вариантов наилучшим образом описывает модель разграничения доступа на основе атрибутов?

- **доступ к ресурсам контролируется через политики, которые используют атрибуты пользователей, ресурсов и окружения. ✓**
- доступ предоставляется пользователям на основе ролей, которые определяются в организации.
- доступ к ресурсам предоставляется на основе секретных ключей, которыми обладают пользователи.
- права доступа определяются исключительно иерархической структурой организации.

(один вариант)

Вопрос 23. Какова основная цель использования модели разграничения доступа на основе псевдонимов в системах информационной безопасности?

- **предоставление пользователям доступа к ресурсам под различными идентичностями для защиты их реальной личности. ✓**
- усиление производительности системы путём уменьшения количества запросов к базе данных.
- упрощение процесса аудита за счет сокращения числа регистрируемых операций.
- автоматическое шифрование данных, сохраняемых в облачном хранилище.

(один вариант)

Вопрос 24. Какое из следующих утверждений наиболее точно описывает модель разграничения доступа на основе возможностей?

- **Доступ к ресурсам предоставляется через прямое предоставление ключей доступа или "возможностей", которые дают пользователю право на выполнение определённых операций с ресурсом. ✓**
- Доступ к ресурсам предоставляется на основе списка контроля доступа.

- ○ Доступ к ресурсам регулируется с помощью централизованной системы, которая требует регулярного переутверждения прав доступа для каждого пользователя.
- ○ Доступ к ресурсам определяется на основе фиксированных уровней безопасности.

(один вариант)

25. Дополните

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа _____ _____ (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Решение: уникального признака

Вопрос 26. Что может быть получено из контрольного журнала после успешной аутентификации?
Ответ:

Решение: Идентификатор

Вопрос 27. Правила разграничения доступа реализуются на основе установленных списков доступа или матриц доступа и должны обеспечивать управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при доступе к:

- ○ техническим средствам, устройствам, объектам файловой системы.
- ○ объектам, создаваемым прикладным и специальным программным обеспечением.
- ○ информации о конфигурации системы защиты информации.
- ○ объектам систем управления базами данных.
- ○ **все варианты верны ✓**

(один вариант)

Вопрос 28. Заполните пропуски. Правила разграничения доступа должны обеспечивать управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при _____ _ _____. *Ответ:*

Решение: входе в систему

Вопрос 29. Какой из нижеперечисленных утверждений наиболее точно описывает управление доступом на основе возможностей?

- ○ **система, где права доступа предоставляются пользователям через токены или ключи, которые представляют собой возможности выполнения определенных действий с ресурсами. ✓**
- ○ система, где доступ к ресурсам контролируется на основе ролей, которые назначаются пользователям.
- ○ система, где доступ к ресурсам регулируется автоматически на основе анализа поведения пользователя в сети.

(один вариант)

Вопрос 30. Типы доступа должны включать операции по:

- ○ созданию
- ○ чтению
- ○ обновлению
- ○ удалению
- ○ **все ответы верны ✓**

Формируемая компетенции	Индикаторы компетенции
ПК-5.В/ПР Способен осуществлять профессиональную деятельность с учетом региональных особенностей и потребностей работодателей.	1. Знает специфику социально-экономического развития и рынка труда в области профессиональной деятельности в своем регионе. 2. Умеет решать профессиональные задачи на предприятиях и в организациях профильной отрасли своего региона.

Вопросы теста для оценки сформированности компетенции ПК-5.В/ПР

Вопрос 1. В информационной системе должны быть установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей:

- ○ определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей)
- ○ объединение учетных записей в группы (при необходимости)
- ○ верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя
- ○ заведение, активация, блокирование и уничтожение учетных записей пользователей
- ○ **Все варианты верны ✓**

(один вариант)

Вопрос 2. В информационной системе должен быть обеспечен запрет предоставления расширенных прав и привилегий *Ответ:*

Решение: Внешним пользователям.

Вопрос 3. Временная учетная запись может быть заведена для пользователя

- ○ на ограниченный срок для выполнения задач, требующих расширенных полномочий
- ○ для проведения настройки, тестирования информационной системы
- ○ организации гостевого доступа
- ○ **Все варианты верны ✓**

(один вариант)

Вопрос 4. В информационной системе должно быть установлено и зафиксировано в организационно-распорядительных документах оператора по защите информации (задокументировано)

- ○ порядок доступа к принтерам и сканерам
- ○ **обеспечено блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе). ✓**
- ○ в информационной системе защита информации регулируется исключительно международными стандартами без учета внутренних документов.
- ○ в информационной системе должно быть установлено антивирусное программное обеспечение без фиксации в организационных документах.

(один вариант)

Вопрос 5. В информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов:

- ○ при входе в информационную систему
- ○ к техническим средствам, устройствам, внешним устройствам
- ○ к объектам, создаваемым общесистемным (общим) программным обеспечением
- ○ к объектам, создаваемым прикладным и специальным программным обеспечением
- ○ **все варианты верны ✓**

(один вариант)

6. В информационной системе обеспечивается для устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за установленный период времени

- автоматическое блокирование.
- возможность разблокирования только администратором или иным лицом, имеющим соответствующие полномочия (роль).
- отправка уведомления администратору системы о необычной активности.
- требование ответа на секретный вопрос перед дальнейшими попытками входа.
- **все варианты верны ✓**

(один вариант)

Вопрос 7. В информационной системе должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы, включающее:

- фильтрацию информационных потоков в соответствии с правилами управления потоками, установленными оператором
- разрешение передачи информации в информационной системе только по маршруту, установленному оператором
- изменение (перенаправление) маршрута передачи информации в случаях, установленных оператором
- запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в случаях, установленных оператором
- **все варианты верны ✓**

(один вариант)

Вопрос 8. Управление информационными потоками должно обеспечивать

- **разрешенный (установленный оператором) маршрут прохождения информации между пользователями, устройствами, сегментами в рамках информационной системы, а также между информационными системами или при взаимодействии с информационно-телекоммуникационными сетями международного информационного обмена на основе правил управления информационными потоками, ✓**
- контроль конфигурации информационной системы, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации).
- информационно-телекоммуникационные сети международного информационного обмена по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из информационной системы и (или) входящие в информационную систему.

(один вариант)

Вопрос 9. В информационной системе обеспечивается автоматическое удаление информации с мобильного технического средства, входящего в состав информационной системы, при

- **Выходе устройства из зоны действия корпоративной сети. ✓**
- Подозрении на взлом устройства.
- При уязвимости в системе безопасности устройства.
- Передаче устройства другому сотруднику.

(один вариант)

Вопрос 10. Заполните пропуск словосочетанием. В информационной системе обеспечивается противодействие автоматизированному подбору паролей с использованием _____ _____, требующих визуального распознавания.

Решение: однократных кодов.

Вопрос 11. В информационной системе должно быть обеспечено предупреждение пользователя в виде сообщения («окна») при ____ _ _____ _____
Ответ:

Решение: входе в информационную систему.

Вопрос 12. Управление информационными потоками должно блокировать передачу защищаемой информации через

- **информационно-телекоммуникационные сети международного информационного обмена по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из информационной системы и (или) входящие в информационную систему. ✓**
- разрешенный маршрут прохождения информации между пользователями, устройствами в рамках информационной системы
- разрешенный маршрут прохождения информации между информационными системами или при взаимодействии с информационно-телекоммуникационными сетями международного информационного обмена
- контроль конфигурации информационной системы, источника и получателя передаваемой информации.

(один вариант)

Вопрос 13. В информационной системе значение числа параллельных сеансов доступа может быть задано

- для информационной системы в целом.
- для отдельных сегментов информационной системы.
- для групп пользователей.
- отдельных пользователей или их комбинаций.
- **Все варианты верны ✓**

(один вариант)

Вопрос 14. Заполните пропуск. В информационной системе пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы должен быть обеспечен доступ с _____ _____, необходимыми для выполнения должностных обязанностей (функций).

Решение: минимальными правами

Вопрос 15. Заполните пропуск. В информационной системе возможность задавать ограничения на число параллельных (одновременных) сеансов (сессий), должна быть предусмотрена основываясь на _____ _____ и (или) принадлежности к роли.

Решение: идентификаторах пользователей

Вопрос 16. Заполните пропуск словосочетанием. Вход в информационную систему и предоставление пользователю возможности работы в информационной системе осуществляются только после подтверждения пользователем _____ _ _____.

Решение: ознакомления с предупреждением.

Вопрос 17. Правила управления информационными потоками включают

- **контроль конфигурации информационной системы, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации). ✓**
- разрешенный маршрут прохождения информации между пользователями, устройствами, сегментами в рамках информационной системы
- информационно-телекоммуникационные сети международного информационного обмена по незащищенным линиям связи.

(один вариант)

Вопрос 18. Заполните пропуск. В информационной системе должен быть определен _____, имеющий права по передаче полномочий по администрированию информационной системы и системы защиты информации другим лицам. И осуществляющий контроль за использованием переданных полномочий (супервизор)

Решение: администратор.

Вопрос 19. В информационной системе ограничение числа параллельных сеансов доступа должно обеспечиваться *Ответ:*

Решение: Для каждой учетной записи.

Вопрос 20. Каковы требования к распределению полномочий в информационной системе, чтобы избежать сосредоточения контроля над системой защиты информации в руках одного должностного лица?

- **Должно быть обеспечено исключение возможности наделения одного лица полномочиями по администрированию системы защиты информации. ✓**
- Должно быть обеспечено назначение одного лица на роль администратора системы защиты информации.
- Должно быть не менее двух лиц с одинаковыми полномочиями по администрированию системы защиты информации.
- Разрешено наделение одного лица полномочиями по администрированию, если это лицо также занимает должность директора по ИБ.

(один вариант)

Вопрос 21. В информационной системе должно быть обеспечено после успешного входа пользователя в информационную систему (завершения процесса аутентификации) оповещение этого пользователя *Ответ:*

Решение: О дате предыдущего входа.

Вопрос 22. В информационной системе должно быть обеспечено предоставление прав и привилегий по доступу к функциям безопасности (параметрам настройки) средств защиты информации *Ответ:*

Решение: Исключительно администратору

Вопрос 23. После успешного входа в информационную систему, то в информационной системе обеспечивается оповещение пользователя

- о количестве неуспешных попыток входа в информационную систему (доступа к информационной системе), зафиксированных с момента последнего успешного входа в информационную систему.
- о количестве успешных и (или) неуспешных попыток входа в информационную систему (доступа к информационной системе), зафиксированных за период времени не менее 7 дней.
- об изменении сведений, относящихся к учетной записи пользователя (в том числе изменении прав доступа), произведенных за период времени не менее, чем с момента предыдущего успешного входа в информационную систему.
- **все варианты верны ✓**

(один вариант)

Вопрос 24. Заполните пропуск. В информационной системе должно быть обеспечено исключение наделения одного должностного лица полномочиями (ролью) по обработке информации и полномочиями (ролью) по _____ информационной системы и (или) ее системы защиты информации

Решение: администрированию.

Вопрос 25. Заполните пропуски. В информационной системе должно быть обеспечено исключение наделения одного должностного лица полномочиями (ролью) по _____ за обеспечением уровня защищенности информации и полномочиями (ролью) по _____ информационной системы.

Решение: контролю, администрированию

Вопрос 26. Заполните пропуск. В информационной системе должно быть обеспечено _____ отдельными должностными лицами полномочий (ролей) пользователей по администрированию системы защиты информации, контролю (мониторингу) за обеспечением уровня защищенности информации, обеспечению функционирования информационной системы

Решение: разделение

Вопрос 27. В информационной системе должно быть обеспечено санкционирование доступа к объектам доступа в соответствии с *Ответ:*

Решение: Разделением ролей

Вопрос 28. Заполните пропуск. В информационной системе должно быть обеспечено фиксирование полномочий в организационно-распорядительных документах по защите информации, т.е. должно производится _____ ролей.

Решение: Документирование

Вопрос 29. В информационной системе должно быть обеспечено - разделение полномочий (ролей) в соответствии с их *Ответ:*

Решение: Должностными обязанностями.

Вопрос 30. В информационной системе в зависимости от получателя информации должно осуществляться наделение трафика

- включение уведомлений пользователей.
- исключение элементов трафика.
- замена элементов трафика.
- **все варианты верны ✓**

(один вариант)