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

Паспорт
расчетно-графической работы

по дисциплине «Безопасность операционных систем», 5 семестр

Методика оценки

Выполнение расчетно-графической работы (далее - РГР) является формой текущей аттестации (контроля) по дисциплине, предусмотренной учебным планом.

Цель РГР: освоение методов настройки и проверки подсистем безопасности Windows, UNIX и Astra Linux Special Edition, анализа событий аудита и реагирования на инциденты информационной безопасности.

Обязательным элементом РГР является решение профессиональных задач администрирования и защиты операционных систем в соответствии с выбранной темой. Проверяются результаты обучения, соотнесённые с индикаторами ОПК-11.3.1, ОПК-12.1 и ОПК-12.3.

Номер задания из перечня п. 4 определяется преподавателем. Каждому студенту задаются индивидуальные исходные данные, состав объектов и параметры учебной системы; они фиксируются в задании на РГР.

РГР выполняется индивидуально на учебном стенде с согласованными исходными данными.

Количество тем и индивидуальных наборов исходных данных обеспечивает каждого обучающегося индивидуальным заданием РГР.

Замена задания РГР осуществляется по согласованию с преподавателем из числа резервных (не занятых) заданий.

Преподаватель осуществляет руководство по выполнению задания, оказывает консультационную помощь и принимает отчет по РГР.

По результатам выполнения РГР выполняется отчет, который состоит из следующих частей:

Титульный лист.

Введение: цель, постановка задания, исходные данные и используемые источники.

Теоретическая часть: описание выбранных принципов, методов и средств.

Практическая часть: разработанное решение, последовательность настройки, положительные и отрицательные проверки, результаты и их анализ.

Выводы или заключение.

Список литературы.

Приложения (при необходимости).

Требования к оформлению:

Объем РГР до 50 страниц машинописного текста формата А4. Шрифт Times New Roman, 12. Формулы набираются в редакторе Math Type. Размещение сканированных формул не допускается. Нумерация страниц сквозная, в нижней части листа по центру арабскими цифрами. Работа должна быть отредактирована, не содержать орфографических, синтаксических и стилевых ошибок.

Отчет в установленные сроки сдается на кафедру для проверки. Преподаватель оценивает качество работы, отмечает положительные стороны и недостатки работы и определяет, допускается ли она к защите. При необходимости преподаватель возвращает РГР студенту для доработки и устанавливает сроки повторного предоставления для проверки. До защиты работы студентом должны быть сделаны необходимые исправления и дополнения по всем замечаниям преподавателя.

При положительном результате оценивания РГР студент её распечатывает, передает на кафедру и защищает до сессии в назначенное преподавателем время.

Защита РГР состоит в индивидуальном устном собеседовании студента с преподавателем. В процессе защиты выявляется уровень знаний студента, степень его самостоятельности при выполнении работы. По результатам защиты студенту выставляется оценка в соответствии с критериями, приведенными в п. 2 настоящего Паспорта.

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

Общие правила выставления оценок текущей аттестации определяются балльно-рейтинговой системой, установленной локальным актом НГТУ.

РГР считается выполненной **на продвинутом** уровне, если все предусмотренные заданием работы выполнены самостоятельно и без ошибок; все разделы РГР выполнены правильно и в полном объеме; работа оформлена в соответствии с требованиями; сдана преподавателю в указанные сроки и не возвращалась для доработки; даны полные и развернутые выводы и рекомендации; на защите студентом даны уверенные и аргументированные ответы. Совокупность запланированных результатов и соотнесенных с ними индикаторов достижения компетенций не содержит пробелов. Закрепленные за РГР компетенции сформированы на продвинутом уровне. Оценка составляет *от 25 до 30 баллов.*

РГР считается выполненной **на базовом** уровне, если все предусмотренные заданием работы выполнены самостоятельно и без существенных ошибок; все разделы РГР выполнены правильно, но есть замечания к полноте предоставления информации; работа оформлена в соответствии с требованиями; сдана преподавателю в указанные сроки и однократно возвращалась студенту для незначительной доработки; в заключении даны выводы и рекомендации; на защите студентом допущены непринципиальные ошибки. Совокупность запланированных результатов и соотнесенных с ними индикаторов достижения компетенций содержит несущественные пробелы. Закрепленные за РГР компетенции сформированы на базовом уровне. Оценка составляет *от 20 до 24 баллов.*

РГР считается выполненной **на пороговом** уровне, если все предусмотренные заданием работы выполнены самостоятельно, но с ошибками, часть из которых носит принципиальный характер; есть замечания к полноте предоставления информации; работа оформлена в соответствии с требованиями; сдана преподавателю, но неоднократно возвращалась студенту для доработки; в заключении даны краткие выводы; защита РГР вызывает у студента серьезные затруднения. Совокупность запланированных результатов и соотнесенных с ними индикаторов достижения компетенций содержит существенные пробелы. Закрепленные за РГР компетенции сформированы на пороговом уровне. Оценка составляет *от 15 до 19 баллов.*

РГР считается **не выполненной** (ниже порогового уровня), если предусмотренные заданием работы выполнены с серьезными ошибками; есть замечания к полноте предоставления информации и оформлению; РГР была сдана преподавателю, но неоднократно возвращалась студенту для доработки, что не привело к улучшению ее качества; РГР не допущена до защиты, что свидетельствует о неудовлетворительном уровне достигнутых студентом результатов. Совокупность запланированных результатов и соотнесенных с ними индикаторов достижения компетенций содержит множественные существенные пробелы. Закрепленные за РГР компетенции не сформированы. Оценка составляет менее 15 баллов.

Шкала оценки

В общей оценке по дисциплине баллы за РГР учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

РГР как форма текущей аттестации (контроля) по дисциплине считается успешно выполненной, если сумма полученных баллов составляет от 15 до 30 баллов включительно.

Примерный перечень тем РГР

1. Разработка политики безопасности учебной информационно-вычислительной системы. Определить активы и угрозы, распределить программно-технические меры Windows и Astra Linux и составить план контроля.
2. Настройка учётных политик Windows. Обосновать параметры паролей и блокирования, применить их в учебной системе и проверить успешные и неуспешные сценарии входа.
3. Разделение административных полномочий Windows. Определить пользовательские роли и привилегии, настроить группы и проверить выполнение разрешённых действий без предоставления избыточных прав.
4. Разграничение доступа к файлам Windows. Реализовать индивидуальную матрицу DACL, исследовать наследование и проверить эффективные права пользователей с различным членством в группах.
5. Исследование разрешающих и запрещающих записей Windows. На учебных каталогах сопоставить несколько вариантов ACL, объяснить итоговый доступ и подготовить рекомендации по устранению конфликтов.
6. Настройка аудита доступа Windows. Выбрать контролируемые объекты и события, настроить политику аудита и SACL, сформировать учебные события и проверить их регистрацию.
7. Анализ событий входа в Windows. Отобрать успешные и неуспешные попытки, выявить отклонения в учебном журнале и предложить порядок реагирования с сохранением исходных сведений.
8. Инвентаризация полномочий Windows средствами PowerShell. Подготовить сценарий получения пользователей, групп и разрешений заданных каталогов, сформировать отчёт и проверить его полноту.
9. Анализ событий безопасности средствами PowerShell. Реализовать отбор и экспорт событий по согласованным признакам, проверить сценарий на учебном журнале и обосновать выводы.
10. Контроль изменений политики Windows. Снять исходное состояние параметров, применить согласованную конфигурацию и сравнить результаты; подготовить порядок безопасного возврата исходных настроек.

11. Разграничение доступа в UNIX. Создать пользователей и группы, реализовать права rwx и дополнительные ACL, проверить влияние маски ACL на эффективные разрешения.
12. Контроль специальных прав UNIX. Исследовать setuid, setgid и sticky на безопасных учебных примерах, определить условия применения и выявить опасные варианты конфигурации.
13. Делегирование административных действий UNIX. Разработать минимальный набор разрешённых операций, проверить работу от имени учебных пользователей и регистрацию использования повышенных полномочий.
14. Аудит дискреционных прав служебного каталога в Astra Linux Special Edition. На готовом стенде сопоставить права каталога и его файлов с заданной политикой, выявить и устранить избыточный доступ через группы и прочих пользователей. Оформить ведомость отклонений и таблицу проверок до и после исправления, подтвердив сохранение разрешённых операций.
15. Исследование расширения дискреционного управления доступом Astra Linux Special Edition. Настроить согласованный сценарий, сопоставить его с базовыми правами и оформить таблицу фактического доступа.
16. Настройка мандатного управления доступом Astra Linux Special Edition. Назначить метки учебным субъектам и объектам, провести разрешённые и запрещённые операции и объяснить результаты.
17. Исследование мандатного контроля целостности Astra Linux Special Edition. Задать уровни целостности, проверить ограничения изменения защищённых объектов и сформулировать требования к полномочиям процессов.
18. Организация аудита Astra Linux Special Edition. Выбрать события доступа и административных изменений, настроить регистрацию на учебном стенде и подготовить разбор полученных записей.
19. Реагирование на учебный инцидент в Windows. По заданному сценарию установить затронутые объекты и учётные записи, сохранить события, обосновать локализацию и проверить восстановление защиты.
20. Реагирование на учебный инцидент в UNIX или Astra Linux. Исследовать ошибочные права либо метки, сопоставить события аудита, выполнить согласованную корректировку и подготовить меры предупреждения повторения.