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

Паспорт
курсовой работы

по дисциплине «Программные средства профессиональной деятельности», 7 семестр

1. **Методика оценки.**

Выполнение курсовой работы (далее – КР) является обязательным видом самостоятельной работы студента по дисциплине, предусмотренным учебным планом.

Основной целью выполнения КР является формирование компетенций и соотнесенных с ними индикаторов по дисциплине «Программные средства профессиональной деятельности», 7 посредством закрепления, углубления и обобщения знаний, полученных студентами за время теоретического обучения и прохождения практик, а также выработка навыков самостоятельного применения знаний и навыков для творческого решения конкретных задач. Выполнение курсовой работы должно способствовать подготовке их к решению более сложной задачи - выполнению выпускной квалификационной работы.

Задачами выполнения курсовой работы является овладение студентами рациональными приёмами сбора, обработки, систематизации информации, применения компьютерных технологий в области программным и программно-аппаратных средств обеспечения безопасности информации в профессиональной деятельности, применения нормативно-законодательной базы и умения оценивать эффективность реализуемых проектов и программ в региональной социально-экономической политике.

Тематика КР соответствует профилю (направленности) подготовки, формируются преподавателями в начале семестра и утверждаются решением кафедры. Количество тем КР достаточно для обеспечения, каждого обучающегося.

Выполнение студентами КР начинается с ознакомления с примерной тематикой. Закрепление тем КР за студентами и назначение научных руководителей утверждается решением кафедры.

Курсовая работа выполняется индивидуально.

Структура курсовой работы :

1. Титульный лист
2. Введение
3. Теоретическая часть
4. Практическая часть
5. Заключение
6. Список литературы и источников
7. Приложения (при необходимости)

Список литературы оформляется в соответствии с библиографическими требованиями в алфавитном порядке и включает от 10 до 20 источников (книг, статей разных авторов, интернет-источников, документов), которые были изучены при выполнении работы.

Требования к оформлению:

Объем КР до *50* страниц машинописного текста формата А4. Шрифт Times New Roman, 12. Нумерация страниц сквозная, в нижней части листа по центру арабскими цифрами. КР должна быть отредактирована, не содержать орфографических, синтаксических и стилевых ошибок.

Законченная курсовая работа предоставляется для проверки в электронном виде в срок, установленный преподавателем. Преподаватель оценивает качество КР с учетом теоретического и практического содержания, достижения ее целей и задач.

Курсовая работа проверяется руководителем работы, который дает письменное заключение по работе — рецензию.

Если при выполнении КР были допущены ошибки, то работа возвращается студенту для исправления выявленных недочетов и затем вновь предоставляется руководителю для проверки. При положительном результате оценивания студент распечатывает работу, передает на кафедру и защищает до сессии в назначенное преподавателем время.

Защита КР проходит публично перед группой студентов.

По результатам защиты студенту выставляется оценка в соответствии с критериями, приведенными в п. 2 настоящего Паспорта.

2. Уровни сформированности компетенций и критерии оценки

В соответствии с балльно-рейтинговой системой НГТУ курсовая работа дисциплине «Программные средства профессиональной деятельности», 7 имеет максимальную оценку 100 баллов.

Курсовая работа выполнен **на продвинутом** уровне, если:

- она выполнена в полном соответствии с заданием, отличается глубиной проработки всех разделов содержательной части, текстовая часть оформлена с соблюдением установленных правил;
- руководитель характеризует деятельность студента положительно (в частности, отмечает его инициативу, самостоятельность, систематичность работы на всех этапах выполнения работы);
- в докладе исчерпывающе, последовательно, четко и логически правильно изложена суть работы и ее основные результаты;
- студент свободно владеет теоретическим материалом, безошибочно применяет его при решении задач, сформулированных в задании;
- в докладе суть работы и ее основные результаты представлены исчерпывающе, последовательно, четко и логически правильно; на все вопросы студент дал обстоятельные и аргументированные ответы, убедительно защищал свою точку зрения;
- компетенции и соотнесенные с ними индикаторы, закрепленные за дисциплиной , по которым выполняется курсовая работа сформированы в полном объеме.

Оценка за выполнение КР составляет *100-87 баллов.*

Курсовая работа выполнен на **базовом** уровне, если:

- соответствует заданию, отличается глубиной проработки всех разделов содержательной части, текстовая часть оформлена с соблюдением установленных правил;
- руководитель характеризует деятельность студента положительно, но с незначительными замечаниями;
- в докладе правильно изложена суть работы и ее основные результаты;
- студент достаточно твердо усвоил теоретический материал и может самостоятельно его применять;
- в докладе суть работы и ее основные результаты представлены полно; на все вопросы студент дал ответы, но их полнота и аргументированность недостаточны;
- компетенции и соотнесенные с ними индикаторы, закрепленные за дисциплиной , по которым выполняется курсовая работа сформированы с небольшими пробелами и соответствуют базовому уровню.

Оценка за выполнение КР составляет *86-73 балла*.

Курсовая работа выполнен **на пороговом** уровне, если:

- выполнена в основном правильно, но без необходимой проработки некоторых разделов;
- в докладе упущены некоторые принципиальные моменты содержательной части работы;
- в докладе представлены суть работы и ее основные результаты; ответы на вопросы вызвали существенные затруднения;
- компетенции и соотнесенные с ними индикаторы, закрепленные за дисциплиной , по которым выполняется курсовая работа сформированы с пробелами и соответствуют пороговому уровню.

Оценка за выполнение КР составляет *72-50 баллов.*

Курсовая работа считается **не выполненной,** если студентом не проработаны важные разделы исследования, допущены принципиальные ошибки, не исправленные после замечаний руководителя курсовой КР . Студент не допущен к защите курсовой работы . компетенции и соотнесенные с ними индикаторы, закрепленные за дисциплиной , по которым выполняется курсовая работа не сформированы.

Оценка составляет *менее 49 баллов*.

3. Шкала оценки.

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

Курсовая работа по дисциплине считается успешно выполненной, если сумма полученных баллов составляет от 100 до 50 баллов включительно.

4. Примерный перечень тем курсовой работы

1. Исследование механизмов обхода систем обнаружения вторжений на основе полиморфных атак
2. Оценка эффективности honeypot-систем при защите корпоративных сетей
3. Анализ уязвимостей в SDN-архитектурах и методы их нейтрализации
4. Оценка устойчивости маршрутизаторов к атакам типа route injection в корпоративных сетях
5. Моделирование DDoS-атаки и оценка производительности средств фильтрации трафика
6. Анализ утечек данных через протокол ARP: механизмы и защита
7. Исследование уязвимостей в протоколах управления сетью (SNMP, NETCONF)
8. Анализ уязвимостей в веб-приложениях с точки зрения управления сессиями
9. Исследование угроз, связанных с использованием iframe в современных веб-сайтах
10. Роль телеметрии в EDR: объём, семантика, политики хранения в российских продуктах
11. Этические и правовые аспекты мониторинга конечных точек в корпоративной среде
12. Открытые форматы данных в SOAR: STIX/TAXII и их адаптация в российской практике
13. Глубина анализа трафика в NGFW: архитектура DPI и её влияние на безопасность
14. Контекстная аналитика в системах обнаружения угроз
15. Корреляция событий в распределённых EDR-средах
16. Нормализация данных в платформах автоматизации
17. Расшифровка зашифрованного трафика в NGFW
18. Влияние DPI на сетевую задержку

19. Интеграция WAF в модель безопасного доступа к облачным сервисам
20. Методы выявления аномалий в сетевом поведении
21. Покрытие уязвимостей в зависимости от языка программирования в системах SAST, DAST, SCA
22. Управление сторонними зависимостями в проектах
23. Выявление C2-коммуникаций по временным меткам
24. Обнаружение перемещения внутри сети после компрометации
25. Ограничения пассивного мониторинга в современных сетях
26. Анализ протоколов для обнаружения скрытых каналов
27. Архитектура управления привилегированным доступом
28. Уровни зрелости автоматизированного реагирования
29. Контекстная семантика данных в системах обнаружения угроз
30. Оценка эффективности детектирования скрытых угроз на основе временной аналитики
31. Политики нормализации данных в условиях несовместимых форматов источников
32. Методология интеграции разнородных систем безопасности в единую SOAR-платформу
33. Политики контроля доступа на основе контекста запроса и поведения пользователя
34. Методы маскировки данных в тестовых базах: безопасность и применимость
35. Исследование уязвимостей в шифровании дисков без криптоалгоритмов
36. Оценка рисков использования shadow IT в организации
37. Исследование изоляции виртуальных машин в гипервизорах VMware и KVM
38. Защита от side-channel атак в виртуализированных средах
39. Сравнительный анализ моделей безопасности SELinux и AppArmor в контексте защиты серверных приложений
40. Методы обнаружения скрытых каналов передачи данных в системах виртуализации
41. Оценка эффективности политик ограничения выполнения кода в пользовательском пространстве
42. Исследование угроз, связанных с использованием сторонних библиотек в промышленных приложениях
43. Оценка эффективности механизмов аудита событий безопасности в распределённых системах
44. Анализ методов обхода контроля за использованием системных вызовов
45. Исследование методов маскировки вредоносной активности в легитимных системных процессах
46. Исследование методов корреляции событий безопасности в распределённых SIEM-системах
47. Исследование влияния шумности журналов на качество обнаружения инцидентов
48. Исследование влияния QoS-политик на возможность маскировки вредоносной активности
49. Анализ возможности корреляции сетевых событий с данными из оперативной памяти после инцидента
50. Анализ особенностей отслеживания перемещения злоумышленника в внутренней сети
51. Оценка эффективности использования NetFlow-данных для реконструкции атаки
52. Анализ применимости passive fingerprinting для идентификации компрометированных узлов
53. Исследование методов идентификации устройств по особенностям сетевого стека
54. Анализ особенностей мониторинга событий в серверах без постоянного подключения к сети
55. Оценка эффективности использования метаданных для повышения контекстной осведомлённости системы безопасности
56. Исследование методов эвристического анализа в песочницах без использования

сигнатур
57. Анализ влияния уровня изоляции среды на достоверность детектирования скрытых действий
58. Исследование влияния уровня интеграции источников данных на скорость обнаружения
59. Анализ особенностей обнаружения вредоносных скриптов в памяти
60. Исследование особенностей детектирования скриптовых атак в памяти без сохранения на диск
61. Исследование влияния объёма трафика на качество обработки в системах NTA
62. Анализ возможностей OSSEC в мониторинге сетевых угроз через корреляцию событий
63. Сравнительный анализ форматов логов Syslog, JSON и CEF в контексте централизованного мониторинга
64. Оценка устойчивости механизмов доставки логов к центральному серверу при сетевых сбоях
65. Анализ эффективности статистического контроля процессов в обнаружении угроз
66. Анализ возможностей обнаружения утечек через скриншоты и печать документов
67. Анализ способов обхода контроля за передачей данных через легитимные SaaS-сервисы
68. Сравнительный анализ подходов к аудиту сессий администраторов без записи экрана
69. Анализ эффективности PAM в средах с высокой динамикой изменения персонала

5. Примерный перечень вопросов к защите курсовой работы

1. Приведите аргументы, которыми руководствовались при выборе темы работы.
2. В чем вы видите актуальность темы исследования?
3. Охарактеризуйте степень разработанности основных проблем, поставленных в вашем курсовом исследовании.
4. Какие теоретические методы при выполнении курсовой работы были использованы?
5. Какие эмпирические методы при выполнении курсовой работы были использованы?
6. В чем вы видите возможности практического применения полученных результатов?
7. Какие механизмы обхода IDS используются в полиморфных атаках и как они эволюционируют?
8. Какие методы детектирования полиморфного вредоносного ПО применяются в современных системах безопасности?
9. Как оценивается эффективность honeypot-систем при защите корпоративных сетей?
10. Какие типы honeypot существуют и в каких случаях они применяются?
11. Какие уязвимости характерны для SDN-архитектур и как они нейтрализуются?
12. Как обеспечивается безопасность контроллера SDN и каналов связи между плоскостями управления и данных?
13. В чём заключается атака типа route injection и как оценивается устойчивость маршрутизаторов к ней?
14. Как моделируются DDoS-атаки для оценки производительности средств фильтрации трафика?
15. Как происходят утечки данных через протокол ARP и какие механизмы защиты применяются ?
16. Какие уязвимости существуют в протоколах управления сетью SNMP и NETCONF и как они эксплуатируются?
17. Какие уязвимости веб-приложений связаны с управлением сессиями?

18. Какие угрозы связаны с использованием iframe в современных веб-сайтах?
19. Какие этические и правовые аспекты необходимо учитывать при мониторинге конечных точек в корпоративной среде?
20. Что такое открытые форматы данных в SOAR (STIX/TAXII) и как они адаптируются в российской практике?
21. Как решается проблема нормализации данных в платформах автоматизации безопасности?
22. Что такое архитектура DPI в NGFW и как она влияет на безопасность сети?
23. Как DPI влияет на сетевую задержку и как решается проблема расшфровки зашифрованного трафика в NGFW?
24. Как интегрируется WAF в модель безопасного доступа к облачным сервисам?
25. Какие методы выявления аномалий в сетевом поведении применяются в современных системах защиты?
26. Как покрытие уязвимостей зависит от языка программирования в системах SAST, DAST, SCA?
27. Как организуется управление сторонними зависимостями в проектах для снижения рисков безопасности?
28. Как выявляются C2-коммуникации по временным меткам и другим признакам?
29. Какие методы обнаружения перемещения злоумышленника внутри сети после компрометации применяются?
30. Какие ограничения имеет пассивный мониторинг в современных сетях?
31. Какие протоколы могут использоваться для организации скрытых каналов передачи данных?
32. Как строится архитектура управления привилегированным доступом в современной организации?
33. Какие уровни зрелости автоматизированного реагирования на инциденты существуют?
34. Что такое контекстная семантика данных в системах обнаружения угроз и как она повышает точность детектирования?
35. Как оценивается эффективность детектирования скрытых угроз на основе временной аналитики?
36. Какие риски несёт использование Shadow IT в организации и как они оцениваются?
37. Как защищаются виртуализированные среды от side-channel атак?
38. В чём различия моделей безопасности SELinux и AppArmor в контексте защиты серверных приложений?
39. Какие методы обнаружения скрытых каналов передачи данных существуют в системах виртуализации?
40. Как оценивается эффективность политик ограничения выполнения кода в пользовательском пространстве?
41. Какие угрозы связаны с использованием сторонних библиотек в промышленных приложениях?
42. Как оценивается эффективность механизмов аудита событий безопасности в распределённых системах?
43. Какие методы обхода контроля за использованием системных вызовов применяются вредоносным ПО?
44. Как вредоносная активность маскируется в легитимных системных процессах и как это выявляется?
45. Какие методы корреляции событий безопасности применяются в распределённых SIEM-системах?
46. Как шумность журналов влияет на качество обнаружения инцидентов?

47. Как QoS-политики могут влиять на возможность маскировки вредоносной активности?
48. Как анализируется возможность корреляции сетевых событий с данными из оперативной памяти после инцидента?
49. Как применяется passive fingerprinting для идентификации компрометированных узлов?
50. Как идентифицируются устройства по особенностям сетевого стека?
51. Какие особенности имеет мониторинг событий на серверах без постоянного подключения к сети?
52. Как метаданные используются для повышения контекстной осведомлённости системы безопасности?
53. Как обнаруживаются вредоносные скрипты в памяти без сохранения на диск (fileless malware)?
54. Как уровень изоляции среды влияет на достоверность детектирования скрытых действий?
55. Какие возможности имеет OSSEC в мониторинге сетевых угроз через корреляцию событий?
56. Чем различаются форматы логов Syslog, JSON и CEF в контексте централизованного мониторинга?
57. Как оценивается устойчивость механизмов доставки логов к центральному серверу при сетевых сбоях?
58. Как статистический контроль процессов используется в обнаружении угроз?
59. Как обнаруживаются утечки через скриншоты и печать документов?
60. Какие способы обхода контроля за передачей данных через легитимные SaaS-сервисы существуют?
61. Какие подходы к аудиту сессий администраторов без записи экрана применяются?
62. Как оценивается эффективность PAM в средах с высокой динамикой изменения персонала?