**НАО «Евразийский национальный университет им. Л. Н. Гумилева»**

**Кафедра** \_\_**Технологии искусственного интеллекта**\_\_

(наименование кафедры)

|  |
| --- |
| **УТВЕРЖДАЮ**  **Декан факультета**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Ф.И.О.**  **(подпись)**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_202\_\_ г.** |

**Рабочая (модульная) учебная программа (Syllabus)**

\_\_\_\_\_\_\_\_ COMS 32007 Информационная безопасность ПО и баз данных\_\_\_\_\_\_\_\_

(код и наименование модуля)

**по дисциплине** \_\_\_\_\_ RBPO 4217 Разработка безопасного программного обеспечения \_\_\_\_\_\_

(код и наименование дисциплины)

**для обучающихся по образовательной программе** \_\_\_\_«6B06109– Администрирование, управления и защита компьютерных систем и сетей на предприятиях»\_

(код и наименование образовательной программы)

**Нур-Султан**

**2022**

Рабочая (модульная) учебная программ (Syllabus) по дисциплине\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_ RBPO 4217 Разработка безопасного программного обеспечения \_\_\_\_\_\_\_\_\_\_\_

(код и наименование дисциплины)

разработана на основании образовательной программы **\_\_\_\_**«6B06109– Администрирование, управления и защита компьютерных систем и сетей на предприятиях»

(код и наименование образовательной программы)

**Разработчик /**

**разработчики** \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Разахова Б.Ш., кандидат технических наук, зав.кафедрой

(подпись) (Ф.И.О., ученая степень, ученое звание, должность)

Рассмотрено на заседании кафедры\_\_ Технологии искусственного интеллекта\_\_\_ протокол №\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_ 202\_\_ г.

Заведующий кафедрой \_\_\_\_\_\_\_\_\_\_\_ \_\_\_ Разахова Б.Ш., к.т.н.\_\_\_\_\_\_\_\_

(подпись) (Ф.И.О., ученая степень, ученое звание)

Одобрено на заседании Учебно-методической комиссии факультета протокол №\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_ 202\_\_ г.

Председатель УМК факультета \_\_\_\_\_\_\_\_\_\_\_ \_\_\_ Сагнаева С.К., к.ф.-м.н.\_\_\_\_\_

(подпись) (Ф.И.О., ученая степень, ученое звание)

**\*Согласовано:**

**Заведующий кафедрой \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \***

(подпись) (Ф.И.О., ученая степень, ученое звание)

*\* Содержание Силлабуса согласовывается с выпускающей кафедрой.*

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

**1. Краткое описание дисциплины**

|  |  |  |
| --- | --- | --- |
| **Цель дисциплины** | **Результаты обучения (РО) по образовательной программе** \* | **Ожидаемые результаты обучения (РО) по дисциплине** |
| Формирование у студентов знаний и умений в области разработки безопасного программного обеспечения. | **АПК1** – проводить анализ действий процессов разработки программного обеспечения (ПО), обосновывать выбор стандартов, методов, инструментариев и языков программирования для разработки ПО, разработка проектной и эксплуатационной документации ПО  **BПК4** – знать требования по интеграции безопасности в жизненный цикл разработки программного обеспечения и лучшие практики минимизации уязвимостей в программном коде; обладать способностью к проведению статической и динамической проверки и оценку безопасности программного приложения. | **Знать** национальные и международные нормативно-правовые документы, регламентирующие организацию защиты ПО в процессе проектирования и разработки  **Обладать способностью** к проведению статической и динамической проверки и оценку безопасности программного приложения  **Уметь** писать безопасный компьютерный код, необходимый для создания и функционирования прикладного программного обеспечения  **Знать** методы поиска уязвимостей и повышения надежности информационных систем на всех стадиях жизненного цикла  **Владеть навыками** разработки проектной и эксплуатационной документации ПО. |

*\*Согласно ОП*

1. **Пререквизиты**

Для освоения данной дисциплины необходимы знания, умения и навыки, приобретённые при изучении следующих дисциплин: Объектно-ориентированное программирование,

Инструментальные средства разработки программ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(название дисциплин)

**Постреквизиты**

Знания, умения и навыки, полученные при изучении дисциплины необходимы для освоения следующих дисциплин: \_\_\_при написания дипломной работы\_\_

(название дисциплин)

**3. Выписка из учебного плана**

Курс \_*4*\_

Семестр\_\_\_7\_\_

Количество кредитов ECTS\_5\_\_\_

|  |  |
| --- | --- |
| **Виды занятий** | **Общее количество часов** |
| Лекции | 15 |
| Практические занятия |  |
| Семинарские занятия | 30 |
| Лабораторные занятия |  |
| Самостоятельная работа обучающегося (СРО) | 105 |
| **Итого** | 150 |

**4. Тематический план дисциплины по модулям**

(в академических часах)

|  |  |
| --- | --- |
| **№ модуля** | **Наименование модуля** |
| 1 |  |
| 2 |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Лекционные занятия** | | | | | |
| **№ недели** | **№ модуля** | **Наименование темы лекции** | **Количество часов** | **Виды и методы обучения** |
| 1 | 1 | Введение в безопасное программирование. Жизненный цикл безопасной разработки программного обеспечения (SSDLC) | **1** | Объяснительно-иллюстративные |
| 2 | 1 | Классификация угроз безопасности программного обеспечения. Формирование требований безопасности к ПО. Определение минимальных приемлемых уровней безопасности. Определение шкалы ошибок и их влияния на безопасность. Проведение оценки рисков безопасности. | 1 | Объяснительно-иллюстративные |
| 3 | 1 | Анализ архитектуры ПО на наличие уязвимостей времени проектирования. Инструментальные средства разработки безопасного ПО. | 1 | Объяснительно-иллюстративные |
| 4 | 1 | Анализ исходных текстов на наличие уязвимостей времени реализации | 1 | Объяснительно-иллюстративные |
| 5 | 1 | Методы защиты ПО от исследования. Классификация средств исследования программ. Способы встраивания защитных механизмов в ПО. Обфускация программ. | 1 | Объяснительно-иллюстративные |
| 6 | 1 | Статический и динамический анализ программ. Статический анализ кода. Динамический анализ программ. Совместное использование статического и динамического анализа программ. | 1 | Объяснительно-иллюстративные |
| 7 | 1 | Автоматизированные средства поиска и устранения уязвимостей ПО. Уязвимости этапа эксплуатации и сопровождения ПО | 1 | Объяснительно-иллюстративные |
| 8 | 2 | Методы обеспечения надежности программ, используемые для контроля их технологической безопасности. | 1 | Объяснительно-иллюстративные |
| 9 | 2 | Подходы к защите разрабатываемых программ от автоматической генерации инструментальными средствами программных закладок | 1 | Объяснительно-иллюстративные |
| 10 | 2 | Способы идентификации вредоносного программного обеспечения. | 1 | Объяснительно-иллюстративные |
| 11 | 2 | Методы и средства обеспечения целостности и достоверности используемого программного кода. Методы защиты программ от несанкциорированных изменений. Схема подписи с верификацией по запросу | 1 | Объяснительно-иллюстративные |
| 12 | 2 | Основные подходы к защите программ от несанкционированного копирования. Краткое описание криптографических средств контроля целостности и достоверности программ | 1 | Объяснительно-иллюстративные |
| 13 | 2 | Методы создания алгоритмически безопасных процедур. Методы создания самотестирующихся и самокорректирующихся программ для решения вычислительных задач | 1 | Объяснительно-иллюстративные |
| 14 | 2 | Тестирование и отладка программных систем. Стратегии и методы тестирования и верификации. Динамический анализ кода программы  Программные средства автоматизации тестирования и верификации. Тестирования на проникновение | 1 | Объяснительно-иллюстративные |
| 15 | 2 | Разработка защищенных Web-приложений | 1 | Объяснительно-иллюстративные |
| **ИТОГО** | | | **15** |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Лабораторные занятия** | | | | | |
| **№ недели** | **№ модуля** | **Наименование тем лабораторных занятий** | **Количество часов** | **Виды и методы обучения** |
| 1 | 1 | Изучить отечественные и зарубежные стандарты в области разработки безопасного программного обеспечения. Составить перечень основныих понятий и определений, используемых в нормативно – правовых документах | 2 | Репродуктивный |
| 2 | 1 | Разработка технических заданий на проектирование эскизных, технических и рабочих проектов подсистем информационной безопасности объекта, с учетом действующих нормативных и методических документов | 2 | Репродуктивный |
| 3 | 1 | Создание и документирование проекта архитектуры программы с учетом требований по безопасности | 2 | Репродуктивный |
| 4 | 1 | Исследование уязвимости этапа реализации. | 2 | Репродуктивный |
| 5 | 1 | Мониторинг активности программ | 2 | Репродуктивный |
| 6 | 1 | Исследование статических анализаторов кода. Применение статического анализатора SonarLint для надежного и безопасного программирования в IDE Eclipse | 2 | Репродуктивный |
| 7 | 1 | Применение специализированных средств выявления уязвимостей в программах | 2 | Репродуктивный |
| 8 | 2 | Оценка технологической безопасности программы на базе метода Нельсона | 2 | Репродуктивный |
| 9 | 2 | Методы защиты программ от потенциально опасных инструментальных средств | 2 | Репродуктивный |
| 10 | 2 | Построить схему системы антивирусной защиты ПО (на примере). | 2 | Репродуктивный |
| 11 | 2 | Применение подписи с верификацией по запрос | 2 | Репродуктивный |
| 12 | 2 | Исследование механизмов защиты программ от незаконного использования и копирования. | 2 | Репродуктивный |
| 13 | 2 | Методы для обнаружения уязвимостей в системе безопасности программного обеспечения буфера. | 2 | Репродуктивный |
| 14 | 2 | Составление тестовых наборов для функционального и структурного тестирования. Тестирование ПО на изменение плоскости атак. | 2 | Репродуктивный |
| 15 | 2 | использование Rational AppScan Developer Edition для управления безопасностью веб-приложений | 2 | Репродуктивный |
| **ИТОГО** | | | 30 |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **СРО** | | | | | |
| **№ недели** | **№ модуля** | **Наименование темы СРО.**  **Сроки сдачи СРО** | **Количество часов** | **Виды и методы обучения** |
| 1 | 1 | Синхронизация программы безопасности с жизненным циклом систем. Подготовить презентацию. | **7** | Частично- поисковый метод |
| 2 | 1 | Изучить междунаровные стандарты составления технической документации по разработке ПО. Подготовить презентацию | **7** | Частично- поисковый метод |
| 3 | 1 | Формирование и утверждения списка разрешенных инструментальных средств разработки, а также используемых стандартов. Подготовить презентацию. | **7** | Частично- поисковый метод |
| 4 | 1 | Обратный инжиниринг приложений | **7** | Частично- поисковый метод |
| 5 | 1 | Анализ возможных плоскостей атак на ПО и противодействие им. Моделирования угроз безопасности ПО. Подготовить доклад | **7** | Исследовательский метод |
| 6 | 1 | Профилирование программ. Доклад. | **7** | Исследовательский метод |
| 7 | 1 | Возможности и способы применения современных автоматизированных средств статического (splint, FindBugs, why3, ...) и динамического (OWASP Zap, BurpSuite, Peach Fuzzer, ...) анализа программ | **7** | Исследовательский метод |
| 8 | 2 | Описание модели Нельсона. | **7** | Исследовательский метод |
| 9 | 2 | Методы индентификации программ и их характеристик | **7** | Исследовательский метод |
| 10 | 2 | Изучить антивирусные программные комплексы. Восстановление зараженных файлов. Профилактика проникновения «троянских программ». | **7** | Исследовательский метод |
| 11 | 2 | Исследование механизмов защиты программ от изучения и изменения | **7** | Исследовательский метод |
| 12 | 2 | Оценка надежности встроенной криптографической защиты типовых программных продуктов. Подготовить презентацию. | **7** | Исследовательский метод |
| 13 | 2 | Ресурсы для обеспечения функциональной безопасности программных средств | **7** | Исследовательский метод |
| 14 | 2 | Фаззинг-тестирование программного обеспечения. Конспект. | **7** | Исследовательский метод |
| 15 | 2 | Изучение программных средств разработки проектной и эксплуатационной документации ПО | **7** | Исследовательский метод |
| **ИТОГО** | | | 105 |  |

**5. Краткая организационно-методическая характеристика дисциплины**

*Виды контроля учебных достижений:*

***Рубежный контроль 1\_\_\_\_\_\_***тестирование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

***Рубежный контроль 2\_\_\_\_\_\_\_\_\_\_\_\_\_*** тестирование ***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

***Итоговый контроль:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***экзамен***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

**Политика и процедуры курса:**

- Обязательное посещение обучающимися всех занятий согласно расписанию;

- Предварительная подготовка к занятиям;

- Своевременное выполнение и сдача СРО;

-Подготовка ко всем видам занятий должна нести самостоятельный, творческий характер;

- Активная работа и проявление креативности во время занятий;

- Участие во всех видах контроля;

- Приверженность Политике академической честности университета.

**6. Учебно-методическая обеспеченность дисциплины**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | **Автор, наименование, издательство, год издания** | Носитель информации | Имеется в наличии (шт.) | |
| В библиотеке | На кафедре |
| 1 | 2 | 3 | 4 | 5 |
| Основная литература | | | | |
| 1 | Казарин О.В., Шубинский И.Б. Надежность и безопасность программного обеспечения. ЮРАЙТ. 2018, 343 с. ISBN:9785534051421 | Учебное пособие |  | https://www.pdfdrive.com/ |
| 2 | Липаев В.В. Надежность и функциональная безопасность комплексов программ реального времени. М: - 2013 , 210 с. | Учебник |  | https://www.pdfdrive.com/ |
| 3 | Лонг Ф., Мохиндра Д. и др. 75 рекомендаций по написанию надежных и защищенных программ. М., СПб., Киев.: Вильямс, 2014. - 256 c. | Учебник |  | https://www.pdfdrive.com/ |
| 4 | Качин К. , Гуерру Р., Родригес Л. Введение в надежное и безопасное распределенное программирование. ДМК. 2011 | Учебник |  | https://www.pdfdrive.com/ |
| 5 | David Hook., Beginning Cryptography with Java. Wrox Press 2012. - 480 р. |  |  | https://www.pdfdrive.com/ |
| Дополнительная литература | | | | |
| 6 | Казарин О.В., Забабурин А.С.. Программно- аппаратные средства защиты информации.-М., Юрайт. 2017.-312 с. | Учебное пособие |  | https://www.pdfdrive.com/ - |
| **Электронные и интернет-ресурсы** | | | | |
| 7 | <https://docs.oracle.com/en/java/javase/11/security/index.html> | | | |
| 8 | <http://citforum.ru> | | | |
| 9 | <https://intuit.ru> | | | |

**7. Система оценки результатов учебных достижений обучающихся**

*Знания, умения и навыки студентов оцениваются по следующей системе*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Оценка по буквенной системе | Цифровой эквивалент баллов | %-ное содержа  ние | Оценка по традиционной системе | Критерии выставления |
| **А** | 4,0 | 95-100 | Отлично | Оценка **А** ставится в том случае, когда дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи. умение демонстрировать понятия, знания требований по интеграции безопасности в жизненный цикл разработки программного обеспечения и методов поиска уязвимостей и повышение надежности информационных систем на всех стадиях жизненного цикла, проводить статическую и динамическую проверку и оценку безопасности программного приложения. Умение писать безопасный компьютерный код, необходимый для создания и функционирования прикладного программного обеспечения. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию обучающихся. |
| **А-** | 3,67 | 90-94 | Оценка **А-** ставится в том случае, когда дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком в терминах науки. Могут быть допущены недочеты в определении понятий, исправленные обучающимся самостоятельно в процессе ответа. |
| **В+** | 3,33 | 85-89 | Хорошо | Оценка **В+** ставится в том случае, когда обучающимся дан полный, развернутый ответ на поставленный вопрос, доказательно раскрыты основные положения темы в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Ответ изложен литературным языком в терминах науки. В ответе допущены недочеты, исправленные обучающимся с помощью преподавателя. |
| **B** | 3,0 | 80-84 | Оценка **В** ставится в том случае, когда дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком в терминах науки. Могут быть допущены недочеты или незначительные ошибки, исправленные обучающимся с помощью преподавателя. |
| **В-** | 2,67 | 75-79 | Оценка **В-** ставится в том случае, когда дан развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен в терминах науки. Однако допущены незначительные ошибки или недочеты, исправленные обучающимся с помощью наводящих вопросов. |
| **С+** | 2,33 | 70-74 | Оценка **С+** ставится в том случае, когда дан полный, но недостаточно последовательный ответ на поставленный вопрос, но при этом показано умение выделить существенные и несущественные признаки и причинно-следственные связи. Ответ логичен и изложен в терминах науки. Могут быть допущены 1–2 ошибки в определении основных понятий, которые обучающийся затруднился исправить самостоятельно. |
| **C** | 2,0 | 65-69 | Удовлетворительно | Оценка **С** ставится в том случае, когда дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Обучающийся не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. Обучающийся может конкретизировать обобщенные знания, доказав на примерах их основные положения только с помощью преподавателя. Речевое оформление требует поправок, коррекции. |
| **С-** | 1,67 | 60-64 | Оценка **С-** ставится в том случае, когда дан неполный ответ, логика, и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, теорий, явлений, вследствие непонимания обучающимся их существенных и несущественных признаков и связей. В ответе отсутствуют выводы. Умение раскрыть конкретные проявления обобщенных знаний не показано. Речевое оформление требует поправок, коррекции. |
| **D+** | 1,33 | 55-59 | Оценка **D+** ставится в том случае, когда дан неполный ответ. Присутствует нелогичность изложения. Обучающий затрудняется с доказательностью. Масса существенных ошибок в определениях терминов, понятий, характеристике фактов, явлений.  В ответе отсутствуют вводы. Речь неграмотна. При ответе на дополнительные вопросы Обучающий начинает осознавать существование связи между знаниями только после подсказки преподавателя. |
| **D** | 1,0 | 50-54 | Оценка **D** ставится в том случае, когда дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Обучающий не осознает связь данного понятия, теории, явления с другими объектами модуля (дисциплины). Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа обучающегося не только на поставленный вопрос, но и на другие вопросы модуля (дисциплины). |
| **FХ** | 0,5 | 25-49 | Неудовлетворительно | Оценке «неудовлетворительно» соответствует буква **FХ, F,** имеющая цифровой эквивалент 0 и процентное содержание 0-49. Данная оценка ставится в том случае, если обучающийся обнаружил пробелы в знании основного материала, предусмотренного программой, не освоил более половины программы модуля (дисциплины), в ответах допустил принципиальные ошибки, не выполнил отдельные задания, предусмотренные формами текущего, промежуточного и итогового контроля, не проработал всю основную литературу, предусмотренную программой. |
| **F** | 0 | 0-24 |