МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 33

УТВЕРЖДАЮ
Руководитель образовательной программы

зав.кафедрой, д.т.н.,проф.
(должность, уч. степень, звание)

С.В. Беззатеев
(инициалы, фамилия)

(подпись)
«20» февраля 2026 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита информации в распределенных информационных системах»
(Наименование дисциплины)

| | |
|---|---|
| Код направления подготовки/ специальности | 10.05.03 |
| Наименование направления подготовки/ специальности | Информационная безопасность автоматизированных систем |
| Наименование направленности/ специализации | Безопасность открытых информационных систем |
| Форма обучения | очная |
| Год приема | 2026 |

Санкт-Петербург– 2026

Лист согласования рабочей программы дисциплины

Программу составил (а)

проф.,д.т.н.,проф. (должность, уч. степень, звание) — 20.02.26 (подпись, дата) — С.Г. Фомичева (инициалы, фамилия)

Программа одобрена на заседании кафедры № 33
«20» февраля 2026 г, протокол № 7

Заведующий кафедрой № 33

д.т.н.,проф. (уч. степень, звание) — 20.02.26 (подпись, дата) — С.В. Беззатеев (инициалы, фамилия)

Заместитель директора института №3 по методической работе

доц.,к.т.н. (должность, уч. степень, звание) — 20.02.26 (подпись, дата) — Н.В. Решетникова (инициалы, фамилия)

Аннотация

Дисциплина «Защита информации в распределенных информационных системах» входит в образовательную программу высшего образования – программу специалитета по направлению подготовки/ специальности 10.05.03 «Информационная безопасность автоматизированных систем» направленности/специализации «Безопасность открытых информационных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ОПК-2 «Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности»

ОПК-12 «Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем»

ОПК-15 «Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем»

ОПК-17 «Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем»

Содержание дисциплины охватывает круг вопросов, связанных с изучением архитектуры распределенных информационных систем (РИС), особенностей защиты информации в РИС, обеспечением безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС, защитой информации на уровне подсистемы управления, защитой информации в каналах связи и особенностями защиты информации в базах данных.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа студента, консультации.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме экзамена (8 семестр).

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа.

Язык обучения по дисциплине «русский »

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины «Защита информации в распределенных информационных системах» для студентов специальности «10.05.03 «Информационная безопасность автоматизированных систем» заключается в приобретении теоретических знаний и формировании практических навыков , связанных с проектированием архитектуры распределенных ИС, разработкой системы защиты информации в РИС, обеспечением безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС, организации защиты информации на уровне подсистемы управления, в каналах связи и в распределенных базах данных.

1.2. Дисциплина входит в состав обязательной части образовательной программы высшего образования (далее – ОП ВО).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП ВО.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

| Категория (группа) компетенции | Код и наименование компетенции | Код и наименование индикатора достижения компетенции |
|---|---|---|
| Общепрофессиональные компетенции | ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности | ОПК-2.З.3 знать типовые прикладные информационные технологии и программное обеспечение, используемое для решения задач профессиональной деятельности, включая системы баз данных, технологии распределенного реестра и искусственного интеллекта |
| Общепрофессиональные компетенции | ОПК-12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем | ОПК-12.В.1 владеть навыками интеграции подсистем, учитывая требования информационной безопасности и защиты информации |
| Общепрофессиональные компетенции | ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный | ОПК-15.З.1 знать методы и инструментальные средства администрирования и контроля систем защиты автоматизированных систем<br>ОПК-15.У.1 уметь осуществлять мониторинг и периодический контроль функционирования средств и систем защиты информации<br>ОПК-15.В.1 владеть навыками использования инструментальных |

| | | |
|---|---|---|
| | мониторинг защищенности автоматизированных систем | средств мониторинга и анализа состояния системы информационной безопасности |
| Общепрофессиональные компетенции | ОПК-17 Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем | ОПК-17.З.1 знать методы защиты информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизации рисков информационной безопасности<br>ОПК-17.В.1 владеть навыками создания механизма оперативного реагирования на угрозы информационной безопасности<br>ОПК-17.В.2 владеть обеспечения непрерывности критических бизнес-процессов |

## 2. Место дисциплины в структуре ОП

Дисциплина может базироваться на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- «Технологии и методы программирования»
- «Основы информационной безопасности»
- «Теория систем и системный анализ»
- «Информационные технологии»
- «Защита информации от утечки по техническим каналам»
- «Методы и средства криптографической защиты информации»
- «Базы данных»
- «Сети и системы передачи информации»
- «Организационное и правовое обеспечение информационной безопасности»
- «Программно-аппаратные средства защиты информации»

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и могут использоваться при изучении других дисциплин:

- «Разработка и эксплуатация автоматизированных систем в защищенном исполнении»
- «Управление информационной безопасностью»
- «Методы и средства проектирования информационных систем»

## 3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

| Вид учебной работы | Всего | Трудоемкость по семестрам |
|---|---|---|
| | | №8 |
| 1 | 2 | 3 |

| | | |
|---|---|---|
| ***Общая трудоемкость дисциплины***, ЗЕ/ (час) | 4/ 144 | 4/ 144 |
| ***Из них часов практической подготовки*** | | |
| ***Аудиторные занятия***, всего час. | 68 | 68 |
| в том числе: | | |
| лекции (Л), (час) | 34 | 34 |
| практические/семинарские занятия (ПЗ), (час) | | |
| лабораторные работы (ЛР), (час) | 34 | 34 |
| курсовой проект (работа) (КП, КР), (час) | | |
| экзамен, (час) | 27 | 27 |
| ***Самостоятельная работа***, всего (час) | 49 | 49 |
| ***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.) | Экз., | Экз., |

## 4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий. Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

| Разделы, темы дисциплины | Лекции (час) | ПЗ (СЗ) (час) | ЛР (час) | КП (час) | СРС (час) |
|---|---|---|---|---|---|
| Семестр 8 | | | | | |
| Раздел 1. Архитектура распределенных ИС<br>Тема 1.1. Топологии распределенных информационных систем<br>Тема 1.2. Топологии организации обмена данными<br>Тема 1.3. Концепции облачных и озер данных<br>Тема 1.4. Архитектура Web-приложений | 6 | | 6 | | 9 |
| Раздел 2.Распределенное управление данными<br>Тема 2.1.Реляционные СУБД<br>Тема 2.2. Нереляционные СУБД | 6 | | 6 | | 10 |
| Раздел 3. Проектирование защищенной РИС<br>Тема 3.1. Определение назначения и функций РИС<br>Тема 3.2. Системный анализ бизнес-процессов<br>Тема 3.3. Проектирование архитектуры РИС<br>Тема 3.4. Проектирование баз данных системы<br>Тема 3.5. Проектирование приложений доступа к данным | 10 | | 10 | | 10 |
| Раздел 4. Основы репликации данных<br>Тема 4.1. Типы репликации<br>Тема 4.2. Агенты репликации<br>Тема 4.3. Особенности репликации данных<br>Тема 4.4. Настройка репликации данных<br>Тема 4.5. Резервирование системных баз данных | 6 | | 6 | | 10 |

| | | | | | |
|---|---|---|---|---|---|
| Раздел 5. Особенности защиты информации в РИС<br>Тема 5.1. Построение системы защиты информации в РИС.<br>Тема 5.2. Особенности защиты информации от непреднамеренных угроз в РИС. Пассивные и активные угрозы безопасности информации в РИС.<br>Тема 5.3. Меры, предпринимаемые для обеспечения безопасности информации в сосредоточенных ИС, механизмы для защиты информации при передаче ее по каналам связи<br>Тема 5.4. Методы и средства, обеспечивающие безопасность информации в защищенной РИС | 6 | | 6 | | 10 |
| Итого в семестре: | 34 | | 34 | | 49 |
| Итого | 34 | 0 | 34 | 0 | 49 |
| | | | | | |

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

| Номер раздела | Название и содержание разделов и тем лекционных занятий |
|---|---|
| **1** | **Архитектура распределенных ИС**<br>Тема 1.1. Топологии распределенных информационных систем (демонстрация слайдов)<br>Тема 1.2. Топологии организации обмена данными (демонстрация слайдов)<br>Тема 1.3. Концепции облачных и озер данных( демонстрация слайдов)<br>Тема 1.4. Архитектура Web-приложений (демонстрация слайдов) |
| **2** | **Распределенное управление данными**<br>Тема 2.1.Реляционные СУБД (демонстрация слайдов)<br>Тема 2.2. Нереляционные СУБД (демонстрация слайдов) |
| **3** | **Проектирование защищенной РИС**<br>Тема 3.1. Определение назначения и функций РИС (демонстрация слайдов)<br>Тема 3.2. Системный анализ бизнес-процессов (демонстрация слайдов)<br>Тема 3.3. Проектирование архитектуры РИС (демонстрация слайдов)<br>Тема 3.4. Проектирование баз данных системы (демонстрация слайдов)<br>Тема 3.5. Проектирование приложений доступа к данным (демонстрация слайдов) |
| **4** | **Основы репликации данных**<br>Тема 4.1. Типы репликации (демонстрация слайдов)<br>Тема 4.2. Агенты репликации (демонстрация слайдов)<br>Тема 4.3. Особенности репликации данных (демонстрация слайдов)<br>Тема 4.4. Настройка репликации данных (демонстрация слайдов)<br>Тема 4.5. Резервирование системных баз данных (демонстрация слайдов) |
| **5** | **Особенности защиты информации в РИС**<br>Тема 5.1. Построение системы защиты информации в РИС. (демонстрация слайдов)<br>Тема 5.2. Особенности защиты информации от непреднамеренных угроз в РИС. (демонстрация слайдов)<br>Тема 5.3. Механизмы для защиты информации при передаче ее по каналам связи (демонстрация слайдов)<br>Тема 5.4. Методы и средства, обеспечивающие безопасность информации в |

| | |
|---|---|
| | защищенной РИС (демонстрация слайдов) |

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

| № п/п | Темы практических занятий | Формы практических занятий | Трудоемкость, (час) | Из них практической подготовки, (час) | № раздела дисциплины |
|---|---|---|---|---|---|
| Учебным планом не предусмотрено | | | | | |
| | | | | | |
| Всего | | | | | |

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

| № п/п | Наименование лабораторных работ | Трудоемкость, (час) | Из них практической подготовки, (час) | № раздела дисциплины |
|---|---|---|---|---|
| Семестр 8 | | | | |
| 1 | «Разработка web-ресурса и desktop-приложения, используемых распределенной базой данных» | 4 | 2 | 1 |
| 2 | «Использование обработчиков исключений при работе с массивами данных» | 4 | 2 | 2 |
| 3 | «Разработка базы данных и подключение desktop-клиента логгирования исключений в распределенной информационной системе» | 4 | 2 | 2,3 |
| 4 | «Разработка Web-клиента мониторинга исключений в распределенной информационной системе» | 4 | 2 | 3 |
| 5 | «Обеспечение целостности информации, Репликация баз данных» | 4 | 2 | 4 |
| 6 | «Реализация методов дешифрования лог-журналов, сформированных защищенным клиентским приложением» | 4 | 2 | 5 |
| 7 | «Парссинг лог-журнала обработчиков исключений» | 4 | 2 | 5 |
| 8 | «Сбор логов событий информационной безопасности в AirSIEM» | 6 | 4 | 2 |
| Всего | | 34 | | |

4.5. Выполнение курсового проекта/ курсовой работы

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

| Вид самостоятельной работы | Всего, час | Семестр 8, час |
|---|---|---|
| 1 | 2 | 3 |
| Изучение теоретического материала дисциплины (ТО) | 20 | 20 |
| Курсовое проектирование (КП, КР) | | |
| Расчетно-графические задания (РГЗ) | | |
| Выполнение реферата (Р) | | |
| Подготовка к текущему контролю успеваемости (ТКУ) | 10 | 10 |
| Домашнее задание (ДЗ) | | |
| Контрольные работы заочников (КРЗ) | | |
| Подготовка к промежуточной аттестации (ПА) | 9 | 9 |
| Всего: | 49 | 49 |

## 5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. разделов 6-11.

## 6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

| Шифр/ URL адрес | Библиографическая ссылка | Количество экземпляров в библиотеке (кроме электронных экземпляров) |
|---|---|---|
| 004<br>Ф 76 | Фомичева, Светлана Григорьевна.<br>Обработка информации в распределенных системах : учебное пособие / С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2020. - 132 с. ; 131 с. : рис. - Библиогр.: с. 123 (17 назв.). - ISBN 978-5-8088-1487-5 : Б. ц. - Текст : непосредственный | 5 |
| 004<br>Б 39 | Беззатеев, Сергей Валентинович (д-р техн. наук, доц.).<br>Программирование задач по обеспечению информационной безопасности : лабораторный практикум / С. В. Беззатеев, С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2020. - 89 с. : рис., табл. - Библиогр.: с. 88 (10 назв.). - Б. ц. - Текст : непосредственный. | 5 |
| 004<br>З-62 | Зима, В. М.<br>Безопасность глобальных сетевых технологий / В. М. | 7 |

| | | |
|---|---|---|
| | Зима, А. А. Молдовян, Н. А. Молдовян. - 2-е изд. - СПб. : БХВ - Петербург, 2015. - 368 с. : рис. - (Мастер систем). - Библиогр.: с. 351 - 353 (31 назв.).- Предм. указ.:с. 354 - 362. - ISBN 978-5-94157-213-7 : 419.00 р. - Текст : непосредственный | |
| 007<br>В 67 | Волкова, В. Н.<br>Теория систем и системный анализ : учебник для академического бакалавриата / В. Н. Волкова, А. А. Денисов ; Нац. исслед. С.-Петерб. гос. политехн. ун-т. - 2-е изд., перераб. и доп. - М. : Юрайт, 2015. - 616 с. : рис. - (Бакалавр. Академический курс). - Предм. указ.: с. 600 - 606. - Имен. указ.: с. 607 - 609. - Библиогр.: с. 610 - 616 (109 назв.). - ISBN 978-5-9916-4783-0 : 870.87 р. - Текст : непосредственный.<br>Имеет гриф УМО высшего образования | 10 |
| 004<br>И 85 | Исаев, Г. Н.<br>Проектирование информационных систем : учебное пособие / Г. Н. Исаев. - 2-е изд., стер. - М. : ОМЕГА-Л, 2015. - 424 с. : рис., табл. - (Высшее техническое образование). - Библиогр.: с. 421 - 424 (61 назв.) . - ISBN 978-5-370-03507-4 : 401.60 р. - Текст : непосредственный.<br>На стр. 7 - 8: Список сокращений | 5 |
| 004<br>Б 24 | Баранова, Е. К.<br>Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. - 3-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2017. - 322 с. : рис., табл. - (Высшее образование). - Библиогр.: с. 313 - 316 (56 назв.). - ISBN 978-5-369-01450-9 (РИОР). - ISBN 978-5-16-011164-3 (ИНФРА-М) : 942.63 р. - Текст : непосредственный.<br>Имеет гриф УМО по образованию в области прикладной информатики | 5 |
| 004.4<br>И 46 | Ильина, Дарья Викторовна.<br>Проектирование и разработка безопасных веб-приложений : учебное пособие / Д. В. Ильина ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2019. - 43 с. : рис. - Библиогр.: с. 42 (2 назв.). - ISBN 978-5-8088-1434-9 : Б. ц. - Текст : непосредственный. | 5 |
| 004.7<br>К 95 | Кучин, Николай Валентинович (доц.).<br>Многоуровневые системы и облачные вычисления : учебное пособие / Н. В. Кучин, А. Ю. Молчанов ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2018. - 136 с. : рис. - Библиогр.: с. 133 (14 назв.). - ISBN 978-5-8088-1250-5 : Б. ц. - Текст : непосредственный | 4 |

## 7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

| URL адрес | Наименование |
|---|---|
| https://pro.guap.ru/ | Материалы для выполнения практических работ, индивидуальные варианты для их выполнения, а также электронный лекционный материал по дисциплине размещаются внутри ЭИОС ГУАП «Интегрированная среда обучения» в течение учебного семестра |

## 8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

| № п/п | Наименование |
|---|---|
| 1 | Электронная информационно-образовательная среда ГУАП «Интегрированная среда обучения» (https://pro.guap.ru/) разработана сотрудниками ГУАП (введена в эксплуатацию приказом ГУАП от 06.06.2017 № 05-215/17), перечень модулей и их функциональное назначение изложены по ссылке https://guap.ru/it/system/iso |
| 2 | Официальный сайт образовательной организации в сети «Интернет» (https://guap.ru/), разработан сотрудниками ГУАП (введен в эксплуатацию Приказом ГУАП от 23.03.2023 № 05-145/23) |
| 3 | LibreOffice 5 (Лицензия LGPLv3) |

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

| № п/п | Наименование |
|---|---|
| 1 | ЭБС Znanium (https://znanium.ru/), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП |
| 2 | ЭБС «Лань» (https://e.lanbook.com/), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП |
| 3 | Электронный каталог библиотеки ГУАП с доступом к базе полнотекстовых изданий (https://lib.guap.ru), доступ через личный кабинет читателя библиотеки ГУАП |

## 9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице12.

Таблица 12 – Состав материально-технической базы

| № п/п | Наименование составной части материально-технической базы | Номер аудитории (при необходимости) |
|---|---|---|
| 1 | Мультимедийная лекционная аудитория: | |

| | | |
|---|---|---|
| | Специализированная мебель; технические средства обучения, служащие для представления учебной информации большой аудитории; набор демонстрационного оборудования. Обеспечен доступ в электронную информационно-образовательную среду ГУАП по точке доступа Wi-Fi. | |
| 2 | Лаборатория компьютерного моделирования:<br>– специализированная мебель;<br>– технические средства обучения, служащие для представления учебной информации; панель интерактивная/телевизор;<br>Лабораторное оборудование: ПЭВМ – «Место рабочее автоматизированное» – 13 шт. Обеспечен доступ в электронную информационно-образовательную среду ГУАП по локальной вычислительной сети. | 52-46, 52-44 (ул. Большая Морская, д.67, лит. А) |
| 3 | Помещение для самостоятельной работы, Интернет-класс. Специализированная мебель, возможность подключения к сети «Интернет» и доступ в электронную информационно-образовательную среду организации. 10 ПК, Принтер лазерный HPLJP4515n, Принтер HP LaserJetEnterprise 600 M602dn. | 14-34 (ул. Большая Морская, д.67, лит. А) |
| 4 | Помещение для самостоятельной работы обучающихся - Читальный зал библиотеки ГУАП: специализированная мебель; персональные компьютеры – 10 шт., обеспечен доступ в электронную информационно-образовательную среду ГУАП по локальной вычислительной сети и точке доступа WiFi, а также к электронно-библиотечным системам, реферативной базе данных Scopus; копировальный аппарат Kyocera KM2035 | 22-19 (ул. Большая Морская, д.67, лит. А) |

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средствдля проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

| Вид промежуточной аттестации | Перечень оценочных средств |
|---|---|
| Экзамен | Список вопросов к экзамену;<br>Экзаменационные билеты*;<br>Задачи;<br>Тесты. |

Примечание: *экзаменационные билеты формируются на основе вопросов и задач таблицы 15.

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 –Критерии оценки уровня сформированности компетенций

| Оценка компетенции | Характеристика сформированных компетенций |
|---|---|
| 5-балльная шкала | |

| Оценка компетенции<br>5-балльная шкала | Характеристика сформированных компетенций |
|---|---|
| «отлично»<br>«зачтено» | Обучающийся:<br>– глубоко и всесторонне усвоил программный материал;<br>– уверенно, логично, последовательно и грамотно его излагает;<br>– опираясь на знания основной и дополнительной литературы, тесно связывает усвоенные научные положения с практической деятельностью направления;<br>– умело обосновывает и аргументирует выдвигаемые им идеи;<br>– делает выводы и обобщения;<br>– свободно владеет системой специализированных понятий.<br>– правильно выполнил от 90% до 100% тестовых заданий**. |
| «хорошо»<br>«зачтено» | Обучающийся:<br>– твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы;<br>– не допускает существенных неточностей;<br>– увязывает усвоенные знания с практической деятельностью направления;<br>– аргументирует научные положения;<br>– делает выводы и обобщения;<br>– владеет системой специализированных понятий.<br>– правильно выполнил от 70% до 89% тестовых заданий**. |
| «удовлетворительно»<br>«зачтено» | – обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы;<br>– допускает несущественные ошибки и неточности;<br>– испытывает затруднения в практическом применении знаний направления;<br>– слабо аргументирует научные положения;<br>– затрудняется в формулировании выводов и обобщений;<br>– частично владеет системой специализированных понятий.<br>– правильно выполнил от 51% до 69% тестовых заданий**. |
| «неудовлетворительно»<br>«не зачтено» | – обучающийся не усвоил значительной части программного материала;<br>– допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении;<br>– испытывает трудности в практическом применении знаний;<br>– не может аргументировать научные положения;<br>– не формулирует выводов и обобщений.<br>– правильно выполнил менее 51% тестовых заданий**. |

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

| № п/п | Перечень вопросов (задач) для экзамена | Код индикатора |
|---|---|---|
| 1 | Архитектура современных распределенных информационных систем и систем их защиты. | ОПК-12.В.1 |
| 2 | Функционал систем управления безопасностью классических и нового поколения | ОПК-15.У.1 |
| 3 | Государственные стандарты, регламентирующие функционирование систем управления безопасностью | ОПК-15.В.1 |
| 4 | Структурные компоненты распределенных информационных систем. Особенности защиты | ОПК-2.3.3 |

| | | |
|---|---|---|
| | информационных ресурсов и процессов | |
| 5 | Компоненты концептуальной модели ИБ. Графическая схема концептуальной модели системы ИБ. | ОПК-17.В.1 |
| 6 | Основные федеральные законы в области защиты информации | ОПК-17.В.2 |
| 7 | Объект и предмет защиты. Основные свойства информации как предмета защиты. Характерные особенности секретной и конфиденциальной информации | ОПК-17.З.1 |
| 8 | Объекты угроз ИБ. Понятие угрозы информации. Основные источники угроз защищаемой информации. Портрет злоумышленника | ОПК-17.З.1 |
| 9 | Уголовная ответственность: предусмотренная при неправомочном использовании информации критической информационной инфраструктуры | ОПК-17.З.1 |
| 10 | Охарактеризуйте свойства информации. Что такое признаковая информация? Почему семантическая информация по отношению к признаковой является вторичной? Какие признаки объектов являются демаскирующими? | ОПК-17.З.1 |
| 11 | Основные способы неправомерного овладения конфиденциальной информацией | ОПК-17.З.1 |
| 12 | Что такое утечка конфиденциальной информации? Как осуществляется утечка конфиденциальной информации? | ОПК-17.В.1 |
| 13 | Классы защищенности информационных систем | ОПК-17.В.1 |
| | Понятия доступности, целостности и конфиденциальности информации. Способы их обеспечения | ОПК-15.З.1 |
| 14 | Понятие кибератаки. Что такое окно опасности? Какие события происходят во время существования окна опасности? | ОПК-17.В.1 |
| 15 | Вектор угроз и его составляющие | ОПК-17.З.1 |
| 16 | Профиль защиты. Приведите стандарты, которые регламентируют разработку профилей защиты. Каково содержание задания по безопасности? | ОПК-17.З.1 |
| 17 | Классифицируйте угрозы ИБ РФ для личности, для общества, для Государства по общей направленности | ОПК-17.З.1 |
| 18 | Критическая информационная инфраструктура. Объекты КИИи субъекты КИИ | ОПК-17.З.1 |
| 19 | Управление рисками. Методики управлению рисками | ОПК-15.З.1 |
| 20 | Каналы утечки информации, Что такое технический канал утечки информации? Охарактеризуйте случайный и организованный канал утечки информации | ОПК-17.В.1 |
| 21 | Направления повседневной деятельности системного администратора, офицера по безопасности, обеспечивающие поддержание работоспособности ИС, а также состав рабочей группы по разработке и внедрению политик информационной безопасности | ОПК-12.В.1 |
| 22 | Информационные ресурсы ФСТЭК для разработчиков, администраторов и экспертов в сфере информационной | ОПК-2.З.3 |

| | | |
|---|---|---|
| | безопасности | |
| 23 | Вредоносное программное обеспечение, Дайте определение «бомбы», «червя», «вируса». Какие негативные последствия в функционировании ИС вызывает вредоносное ПО? | ОПК-15.3.1 |
| 24 | Что такое идентификация? Дайте толкование понятия «аутентификация». Из-за каких причин затруднена надежная идентификация? | ОПК-15.3.1 |
| 25 | Средств защиты информации (СЗИ), их классификация. Классы защищенности СЗИ. | ОПК-17.3.1 |
| 26 | Особенности защиты биометрической информации | ОПК-17.3.1 |
| 27 | Системы контроля и управления доступом. Что такое матрица доступа? Какая информация анализируется при принятии решения о предоставлении доступа? | ОПК-15.3.1 |
| 28 | Системы протоколирования. Прокомментируйте особенности применения данного сервиса безопасности. Какие средства автоматизации существуют для мониторинга событий безопасности? | ОПК-15.3.1 |
| 29 | Основная задача аудита, как сервиса безопасности. Функциональность SIEM-систем? | ОПК-15.3.1 |
| 30 | Экранирование как сервис безопасности РИС. Что такое firewall и как он функционирует? | ОПК-15.3.1 |
| 31 | Для каких целей служит сервис анализа защищенности? В чем заключается специфика управления, как сервиса безопасности? | ОПК-15.3.1 |
| 32 | Какие нормативные акты и стандарты регламентируют деятельность по поверке (оценке) уровня защищенности? Что такое оценочный уровень доверия? | ОПК-15.3.1 |

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

| № п/п | Перечень вопросов (задач) для зачета / дифф. зачета | Код индикатора |
|---|---|---|
| | Учебным планом не предусмотрено | |

Перечень тем для выполнения курсового проекта/ курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для выполнения курсового проекта / курсовой работы

| № п/п | Примерный перечень тем для выполнения курсового проекта/ курсовой работы |
|---|---|
| | Учебным планом не предусмотрено |

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

| № п/п | Примерный перечень вопросов для тестов | Код индикатора |
|---|---|---|
| 1 | К какой разновидности моделей управления доступом относится модель Белла-Ла Падулы?<br>а) модель дискреционного доступа; | ОПК-15.3.1 |

| | | |
|---|---|---|
| | б) модель мандатного доступа;<br>в) ролевая модель. | |
| 1 | Как называются угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.? | ОПК-17.З.1 |
| 3 | К каким мерам защиты относится политика безопасности?<br>а) к административным;<br>б) к законодательным;<br>в) к программно-техническим;<br>г) к процедурным. | ОПК-17.З.1 |
| 4 | В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу?<br>а) ACL;<br>б) списки полномочий субъектов;<br>в) атрибутные схемы. | ОПК-15.З.1 |
| 5 | Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений?<br>а) целостность;<br>б) апеллируемость;<br>в) доступность;<br>г) конфиденциальность;<br>д) аутентичность | ОПК-12.В.1 |
| 6 | К основным принципам построения системы защиты АИС относятся:<br>а) открытость;<br>б) взаимозаменяемость подсистем защиты;<br>в) минимизация привилегий;<br>г) комплексность;<br>д) простота | ОПК-17.З.1 |
| 7 | Какие из следующих высказываний о модели управления доступом RBAC справедливы?<br>а) с каждым субъектом (пользователем) может быть ассоциировано несколько ролей;<br>б) роли упорядочены в иерархию;<br>в) с каждым объектом доступа ассоциировано несколько ролей ;<br>г) для каждой пары «субъект-объект» назначен набор возможных разрешений | ОПК-15.З.1 |
| 8 | . Диспетчер доступа...<br>а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа;<br>б) ... использует атрибутные схемы для представления матрицы доступа;<br>в) ... выступает посредником при всех обращениях субъектов к объектам;<br>г) ... фиксирует информацию о попытках доступа в системном журнале; | ОПК-12.В.1 |
| 9 | Какие предположения включает неформальная модель нарушителя?<br>а) о возможностях нарушителя;<br>б) о категориях лиц, к которым может принадлежать нарушитель;<br>в) о привычках нарушителя;<br>г) о предыдущих атаках, осуществленных нарушителем; | ОПК-2.З.3 |

| | | |
|---|---|---|
| | д) об уровне знаний нарушителя | |
| 10 | Что представляет собой доктрина информационной безопасности РФ?<br>а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности;<br>б) федеральный закон, регулирующий правоотношения в области информационной безопасности;<br>в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов;<br>г) совокупность официальных взглядов на цели, задачи, принципы и основные на- правления обеспечения информационной безопасности Российской Федерации | ОПК-2.3.3 |
| 11 | К какому виду мер защиты информации относится утвержденная программа работ в области безопасности?<br>а) политика безопасности верхнего уровня;<br>б) политика безопасности среднего уровня;<br>в) политика безопасности нижнего уровня;<br>г) принцип минимизации привилегий;<br>д) защита поддерживающей инфраструктуры. | ОПК-17.3.1 |
| 12 | Какие из перечисленных ниже угроз относятся к классу преднамеренных?<br>а) заражение компьютера вирусами;<br>б) физическое разрушение системы в результате пожара;<br>в) отключение или вывод из строя подсистем обеспечения функционирования вы- числительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);<br>г) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;<br>д) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;<br>е) вскрытие шифров криптозащиты информации | ОПК-17.3.1 |

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

| № п/п | Перечень контрольных работ |
|---|---|
| | Не предусмотрено |

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

## 11. Методические указания для обучающихся по освоению дисциплины

11.1. Методические указания для обучающихся по освоению лекционного материала .

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимися лекционного материала:

– получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;

– получение опыта творческой работы совместно с преподавателем;

– развитие профессионально-деловых качеств, любви к предмету и самостоятельного творческого мышления.

– появление необходимого интереса, необходимого для самостоятельной работы;

– получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;

– научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);

– получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала (https://pro.guap.ru/inside#subjects/2403842):

- Изложение лекционного материала;
- Представление теоретического материала преподавателем в виде слайдов;
- Освоение теоретического материала по практическим вопросам;
- Список вопросов по теме для самостоятельной работы студента

11.2. Методические указания для обучающихся по участию в семинарах = *учебным планом не предусмотрено*

11.3. Методические указания для обучающихся по прохождению практических занятий - *учебным планом не предусмотрено*

11.4. Методические указания для обучающихся по выполнению лабораторных работ;

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач обучающегося:

– приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;

– закрепление, развитие и детализация теоретических знаний, полученных на лекциях;

– получение новой информации по изучаемой дисциплине;

– приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

**Лабораторная работа № 1** «Разработка web-ресурса и desktop-приложения, используемых распределенной базой данных»

Цель работы: Основная цель данного занятия – подготовка web-ресурса и desktop приложения для их дальнейшего подключения к распределенным базам данных

Задание к лабораторной работе №1 –

1) Создать статический макет сайта на примере Интернет-магазина, т.е. задать структуру сайта, задать разметку основным страницам и шаблонам, определить необходимые CSS –классы

2) Получить навыки работы с битовыми операциями в объектно-ориентированной среде программирования (например, Microsoft Visual Studio 2019). Создать клиентские приложение с использованием Windows Forms на одном из языков C#/Python/C++/J.

Порядок выполнения работы

1) Создать статический макет сайта

2) Разработать в Windows Forms Desktop-проект, в соответствии с индивидуальным вариантом с выводом промежуточных результатов, добавить обработчики исключений.

2) Разработать функционал формирования лог-журнала обработки

Исключений

Структура и форма отчета о лабораторной работе и требования к оформлению отчета о лабораторной работе:

Оформить отчет по лабораторной работе, содержащий: титульный лист, название, номер и цель работы, постановку задачи, листинг программных модулей, распечатку результатов, распечатку изображения форм, используемых в программе.

Ссылка на требования к лабораторной работе - https://pro.guap.ru/inside#tasks/60111

**Лабораторная работа № 2** «Использование обработчиков исключений при работе с массивами данных»

Цель работы: Получить навыки работы обработки исключений при работе с массивами данных, формируемыми в различных потоках процесса и режимах.

Порядок выполнения работы:

1) Создать программный проект с защищенным интерфейсом пользователя. Обработанные исключения фиксировать в текстовом файле с указанием даты и времени проявления исключений, сообщения исключения и стека вызовов.

2) Создать программу, выполняющую персональное задание в соответствии с заданным вариантом, причем ввод и вывод массивов производить сиспользованием компонента dataGridView. Интерфейс пользователя должен предлагать выбор способа формирования массива (случайно, случайно с заданной частотой, вручную)

3) При формировании длинных массивов в dataGridView выводить первые Nэлементов массива, где N задается пользователем.

4) Преобразования элементов массива выполнять параллельно, используя потоки.

Структура и форма отчета о лабораторной работе и требования к оформлению отчета о лабораторной работе

Оформить отчет по лабораторной работе, содержащий: титульный лист, название, номер и цель работы, постановку задачи, алгоритм решения для каждого программного модуля, листинг программных модулей, распечатку результатов, распечатку изображения форм, используемых в программе.

Ссылка на требования к лабораторной работе - https://pro.guap.ru/get-task/5723d0ccf18694ef7cace58ed56bcfef

**Лабораторная работа № 3** «Разработка базы данных и подключение desktop-клиента логгирования исключений в распределенной информационной системе»

Цель работы: Изучить принципы построения приложений, являющихся источниками данных в распределенных информационных системах, научиться использовать методы проектирования приложений доступа к данным, базируясь на принципах Code-First. Освоить механизмы Entity Framework для проектирования desktop-клиентов РИС.

Порядок выполнения работы:

1) Изучить материалы методических рекомендаций к ЛР 3, размещенные в личном кабинете.

2) В соответствии с заявленной в методических рекомендациях функциональностью, разработать клиент-серверную БД и подключить к ней desktop-клиент, являющийся комплексным проектом логгирования исключений, возникающих в ходе эксплуатации различных форм проекта поддержки лабораторных работ по дисциплинам в области информационной безопасности.

3) Desktop-клиент в зависимости от действий пользователя должен уметь переходить в режим записи исключений в базу данных системы AirLogger (сущность UserException) в реальном масштабе времени.

4) Разработать дополнительный функционал проекта в соответствии с индивидуальным вариантом.

Структура и форма отчета о лабораторной работе и требования к оформлению отчета о лабораторной работе: Оформить отчет по лабораторной работе, содержащий: титульный лист, название, номер и цель работы, постановку задачи, алгоритм решения для каждого программного модуля, листинг программных модулей, распечатку результатов, распечатку изображения форм, используемых в программе.

Ссылка на требования к лабораторной работе - https://pro.guap.ru/get-task/4e4032eafd4f08331e2771e525ea4344

**Лабораторная работа № 4** «Разработка Web-клиента мониторинга исключений в распределенной информационной системе»

Цель работы: Изучить принципы построения MVC-решений, позволяющих распределить бизнес-логику в распределенных информационных системах, научиться использовать методы проектирования приложений доступа к данным, базируясь на принципах Model-First. Освоить механизмы Entity Framework для проектированияWeb-клиентов РИС.

Порядок выполнения работы:

1) Изучить материалы лекций, размещенные в личном кабинете.

2) В соответствии с заявленной в лекциях функциональностью, разработать Web-клиент, использующий ASP.NET Core MVC подходы разработки распределенных систем.

3) Web-клиент должен обеспечивать возможность удаленного мониторинга таблицы UserExceptions разработанной ранее архитектуры БД, а также поддержку вызова CRUD-операций (create, read, update, delete) над данной таблицей.

4) Локализовать интерфейс Web-клиента (на русском языке должны бвть все его элементы)

5) Разработать дополнительный функционал проекта в соответствии с индивидуальным вариантом.

6) Заполнить таблицы базы данных AirLogger осмысленными данными (длявсех таблиц БД минимум по 3-4 записи)

Структура и форма отчета о лабораторной работе и требования к оформлению отчета о лабораторной работе: Оформить отчет по лабораторной работе, содержащий: титульный лист, название, номер и цель работы, постановку задачи, алгоритм решения для каждого программного модуля, листинг программных модулей, распечатку результатов, распечатку изображения форм, используемых в программе

Ссылка на требования к лабораторной работе - https://pro.guap.ru/get-task/a92300e8f9551af8e9419d4b6424e113

**Лабораторная работа № 5** «Обеспечение целостности информации, Репликация баз данных»

Цель работы: Получить навыки работы по обеспечению целостности информации с помощью технологий репликации распределенных баз данных. Создать защищенные клиентские приложения с использованием Windows Forms и MVC ASP.Net на языке C#, осуществляющее доступ к распределенной базе данных СУБД Microsoft SQL Server 2016/2019 с поддержкой функций репликации. .

Порядок выполнения работы

Ход работы фиксировать скриншотами (при невозможности продемонстрировать выполнение работы в университете – записать видео выполнения лабораторной работы)

1) Выполнить развертывание телекоммуникационной инфраструктуры, включающей в себя не менее двух хостов (физических и/или виртуальных) на базе операционных систем Windows 10, Windows Server 2012/2016/2019 или Linux Ubuntu, на каждом из которых установить СУБД Windows SQL Server 2016/2019 Developer и SQL Server Management Studio (ссылка https://www.microsoft.com/enus/sql-server/sql-server-downloads)

2) Открыть для входящего трафика должны быть открыты следующие порты:

TCP 1433, 1434, 2383, 2382, 135, 80, 443;

UDP 1434

3) На хостах 1 и 2 создать учетную запись для пользователя mssql.

4) На хосте 2 развернуть клиентские приложения информационной системы AirLogger и обеспечить доступ к базе данных этой системы.

5) На хостах 1 и 2 запустить службу агента SQL Server

6) На хостах 1 и 2 выполнить настройку пользователей mssql для MS SQL Server

7) На хост 1 импортировать базу данных ИС AirLogger

8) На хостах 1 и 2 выполнить настройку серверов MS SQL Server (В разделе «Роли сервера» установите флаг рядом с ролью dbcreator и sysadmin, В членство в «Роли базы данных» БД AirLogger, отметьте флаг db_owner)

9) На хосте 1 выполнить настройку репликации базы данных транзакциями.

10) На хосте 1 выполнить настройку распространителя

11) На хосте 1 выполнить настройку издателя

12) На хосте 1 выполнить выталкивающую (push) настройку подписчика

13) На хосте 1 запустить монитор репликации

14) Выполнить проверку работы репликации

15) Изменить тип поддерживаемой репликации (для юношей – репликацию транзакциями изменить на репликацию слиянием. Для девушек - репликацию транзакциями изменить на репликацию моментальными снимками)

16) Повторно выполнить проверку работы репликации

17) Оформить отчет по лабораторной работе

Структура и форма отчета о лабораторной работе и требования к оформлению отчета о лабораторной работе: Оформить отчет по лабораторной работе, содержащий: титульный лист, название, номер и цель работы, постановку задачи, алгоритм решения для каждого программного модуля, листинг программных модулей, распечатку результатов, распечатку изображения форм, используемых в программе

Ссылка на требования к лабораторной работе - https://pro.guap.ru/get-task/775cfc20a2c25c34af673c460cd910e8

**Лабораторная работа № 6** «Реализация методов дешифрования лог-журналов, сформированных защищенным клиентским приложением»

Цель работы: Получить навыки работы с криптографическими алгоритмами в среде программирования Microsoft Visual Studio 2019. Реализовать декодирование лог-журналов защищенного клиентского приложения с использованием Windows Forms на языке C#.

Порядок выполнения работы

1) Проанализировать шаблоны частных политик безопасности. Выделить политики, актуальные для процессов управления доступом. Адаптировать выбранные политики для обеспечения требований «сильных. паролей». Добавленные и/или адаптированные правила отобразить в частных политиках жирным шрифтом.

2) Разработать функционал формирования декодирования лог-журнала обработки исключений, который был подвергнут шифрованию в соответствии с заданным вариантом при выполнении требований адаптированных частных политик безопасности информации.

3) Для осуществления процессов шифрования/дешифрования использовать соответствующие пункты главного меню главной формы проекта. Форма авторизации и ввода (формирования) ключа шифрования должна быть модальной, а сам ключ формироваться в соответствии с правилами «сильных ключей».

4) В статусной строке главной формы фиксировать время, затраченное на процессы шифрования/дешифрования.

Структура и форма отчета о лабораторной работе и требования к оформлению отчета о лабораторной работе: Оформить отчет по лабораторной работе, содержащий: титульный лист, название, номер и цель работы, постановку задачи, алгоритм решения для каждого программного модуля, листинг программных модулей, распечатку результатов, распечатку изображения форм, используемых в программе.

Ссылка на требования к лабораторной работе - https://pro.guap.ru/get-task/453d2f9c96f6175197648c9cb089ffaa

**Лабораторная работа № 7** «Парссинг лог-журнала обработчиков исключений»

Цель работы: Получить навыки работы с регулярными выражениями, поиска сигнатур в логе обработки исключений, замены и извлечения «подозрительных» словоформ.

Порядок выполнения работы:

1) В проекте с лабораторными работами добавить форму с функционалом парссинга текста. Доработать обработчик кнопки «Выделить включения» так, чтобы при НОВОМ выборе сигнатуры в comdoBox ВЫБРАННАЯ сигнатура отображалась в richBox иным цветом.
2) Добавить функционал, когда при добавлении в richBox текста не из файла (ввод текста пользователем) осуществлялся поиск последовательно выбираемых сигнатур.
3) Для сформированного лог-журнала на ПЕРВОЙ форме проекта определить, в каких формах (виджетах) появлялись исключения и по сколько раз они появились в каждой форме (включения наименований этих форм в лог-журнале выделить цветом)
4) Выполнить задание в соответствии с индивидуальным вариантом.
5) Реализовать парссинг сохраненных лог-журналов в многопоточном режиме (для каждого лог-файла создавать свой поток). Определить время парссинга каждого журнала и всех выбранных журналов.

Структура и форма отчета о лабораторной работе и требования к оформлению отчета о лабораторной работе: Оформить отчет по лабораторной работе, содержащий: титульный лист, название, номер и цель работы, постановку задачи, алгоритм решения для каждого программного модуля, листинг программных модулей, распечатку результатов, распечатку изображения форм, используемых в программе.

Ссылка на требования к лабораторной работе -. https://pro.guap.ru/inside#tasks/81454

**Лабораторная работа № 8** «Сбор логов событий информационной безопасности в AirSIEM»

Цель лабораторной работы разработать систему, которая позволяет анализировать регистрируемые в защищаемой инфраструктуре события, поступающие от различных

источников, и обнаруживать атаки/сценарии атак/подозрительные действия/отклонения от нормы, формируя при необходимости соответствующие инциденты безопасности.

Задание к лабораторной работе №8

1) Развернуть SIEM-экосистему, используя проект AirSIEM (образ диска содержит AirSIEM, развернуую на Windows 7)

2) Развернуть AirSIEM, используя на Windows 10)

3) Реализовать подсистему сбора и хранения поступающих событий безопасности;

4) Оформить отчет по лабораторной работе.

Структура и форма отчета о лабораторной работе и требования к оформлению отчета о лабораторной работе: Оформить отчет по лабораторной работе, содержащий: титульный лист, название, номер и цель работы, постановку задачи, скриншоты развертывания AirSIEM

Ссылка на требования к лабораторной работе - https://pro.guap.ru/inside#tasks/82675

11.5. Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

В процессе выполнения самостоятельной работы у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет ему развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихсяявляются:

– учебно-методический материал по дисциплине;

– методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

11.6. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

Текущий контроль включает следующие формы:

– Устный опрос (коллоквиум, собеседование)

– Письменные работы (тестирование)

– Лабораторные работы

– Проектная деятельность (рефераты, доклады, презентации)

Критерии оценивания

Оценка выставляется на основе демонстрации обучающимся следующих компетенций:

– Оценка «Отлично» (высокий уровень): глубокое знание материала, логичное изложение, умение решать нестандартные задачи, аргументированные ответы.

– Оценка «Хорошо» (продвинутый уровень): твердое знание материала, грамотное изложение, выполнение практических заданий без принципиальных ошибок, небольшие неточности при ответах.

– Оценка «Удовлетворительно» (пороговый уровень): знание базовых положений, затруднения при самостоятельном анализе, наличие ошибок в вычислениях или логике, неуверенные ответы.

– Оценка «Неудовлетворительно» (критический уровень): отсутствие базовых знаний, невыполнение обязательных практических заданий, отказ от ответа.

Порядок ликвидации задолженностей

– Обучающийся обязан проходить все формы контроля в установленные сроки.

– В случае пропуска по уважительной причине (болезнь, подтвержденная справкой), сроки прохождения переносятся.

– При неудовлетворительной оценке или неуважительном пропуске обучающийся обязан отработать задолженность в часы консультаций преподавателя до начала сессии.

11.7. Методические указания для обучающихся по прохождению промежуточной аттестации.

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Порядок проведения аттестации:

1. Допуск к аттестации. Студент обязан выполнить все практические, лабораторные и курсовые работы. Все текущие контроли должны быть сданы в срок.
2. Подготовка к контролю. Преподаватели выдают перечень вопросов и заданий. Кафедра организует консультации перед экзаменом.
3. Проведение испытания. Аттестация проходит по утвержденному расписанию сессии. Билет содержит теоретические вопросы и практические задачи.
4. Выставление отметки. Преподаватель оценивает ответ сразу после экзамена.

Критерии выставления оценок на экзамене определяются уровнем усвоения материала, глубиной знаний и умением применять их на практике. При этом используется классическая четырехбалльная система отчетов.

Расшифровка экзаменационных оценок

– «Отлично» (5). Студент демонстрирует глубокое и полное знание материала. Свободно владеет терминологией, логично излагает ответ, не допускает ошибок. Легко решает сложные практические задачи и связывает теорию с практикой.

– «Хорошо» (4). Студент твердо знает материал и грамотно его излагает. Ответ правильный по существу, но могут быть мелкие неточности или пропуски. Практические задания выполняются уверенно, но с незначительными недочетами.

– «Удовлетворительно» (3). Студент знает только основной материал, путается в деталях и терминах. Ответ поверхностный, нарушена логика изложения. Практические задачи вызывают серьезные затруднения и решаются только с помощью наводящих вопросов преподавателя.

– «Неудовлетворительно» (2). Студент имеет грубые пробелы в базовых знаниях. Не может ответить на основные вопросы и не справляется с практическими заданиями. Оценка означает, что курс не освоен, и ведет к академической задолженности.

Сравнение оценок по ключевым критериям

| Оценка | Понимание теории | Практические навыки | Самостоятельность |
|---|---|---|---|
| Отлично | Полное, системное | Безошибочное | Полная |

| | | | |
|---|---|---|---|
| | | выполнение | самостоятельность |
| Хорошо | Твердое, без грубых ошибок | Выполнение с мелкими недочетами | Высокая самостоятельность |
| Удовлетворительно | Поверхностное, фрагментарное | Выполнение с подсказками | Требуется помощь |
| Неудовлетворительно | Отсутствует | Задания не выполнены | Не справляется |

Лист внесения изменений в рабочую программу дисциплины

| Дата внесения изменений и дополнений. Подпись внесшего изменения | Содержание изменений и дополнений | Дата и № протокола заседания кафедры | Подпись зав. кафедрой |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |