Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Смоленский государственный университет»

Кафедра прикладной математики и информатики

«Утверждаю»
Проректор по учебно-
методической работе
_____Устименко Ю.А.
«8» сентября 2021 г.

Рабочая программа дисциплины
Б1.В.ДВ.02.01 ЗАЩИТА ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

Направление подготовки: **01.04.02 Прикладная математика и информатика**
Направленность (профиль): **Прикладные интернет - технологии**
Форма обучения: очная
Курс – 1
Семестр – 1
Всего зачетных единиц – 2, часов – 72

Форма отчетности: зачет – 1 семестр

Программу разработал
кандидат технических наук, доцент Т.А. Самойлова

Одобрена на заседании кафедры
«1» сентября 2021 г., протокол № 1

Смоленск
2021

1. Место дисциплины в структуре ОП

Дисциплина «Защита информации в сети интернет» относится к дисциплинам по выбору. Она изучается в 1 семестре и является вспомогательной для изучения таких дисциплин, как «Проектирование сетевых информационных систем», «Разработка веб - сервисов для мобильных приложений» и др.

При изучении данной дисциплины необходимы компетенции студентов, сформированные при изучении таких дисциплин, как «Информационные системы», «Базы данных», «Защита информации». В курсе рассматриваются вопросы криптографической защиты информационных систем, а также способы защиты от хакерских атак для веб - приложений информационных систем. Она знакомит магистра с системой основных типов и способов защиты информации; обеспечивает приобретение магистрами умения проектировать системы защиты информации; овладение современными программными и аппаратными средствами защиты информации. Приобретенные в результате изучения дисциплины знания помогут магистру выбрать направление будущих научных исследований.

Изучение курса основано на традиционных методах высшей школы, тесной взаимосвязи со смежными курсами, а также на использовании современного программного обеспечения защиты веб – приложений.

2. Планируемые результаты обучения по дисциплине

Компетенция	Индикаторы достижения *(в соответствии с разделом 7 общей характеристики ОП ВО)*
ПК-1. Способность осуществлять поиск, анализ, систематизацию научной информации в области прикладной математики и информатики для реализации научно-исследовательских проектов и решения прикладных задач	**Знать**: основные понятия и направления защиты информации в сети интернет; законодательство Российской Федерации в области защиты информации; современные методы и средства защиты информации в сетевых информационно-телекоммуникационных системах; архитектуру защищённых информационных систем. **Уметь**: разрабатывать политику информационной безопасности в сети интернет; проводить оценку угроз безопасности объекта информатизации; реализовывать простые информационные технологии реализующие методы защиты информации; применять методики оценки уязвимости в информационно - телекоммуникационных сетях. **Владеть**: методами и средствами защиты информации в сетях интернет.
ПК-3. Способность разрабатывать программное обеспечение, в том числе драйверы устройств, компиляторы, загрузчики, сборщики, системные утилиты	**Знать**: методы и алгоритмы, используемые для решения задач защиты информации в сети интернет; концептуальные и теоретические модели проектирования программного обеспечения средств защиты. **Уметь**: самостоятельно находить и/или разрабатывать алгоритмы для решения проблем защиты информации в сети интернет, модернизировать их для конкретной задачи, применять различные методы и приемы проектной и производственно-технологической деятельности. **Владеть**: навыками создания алгоритмического описания задач защиты веб - приложений; навыками программирования алгоритмов

	защиты информации в сети интернет от хакерских атак.

3. Содержание дисциплины

В дисциплине «Защита информации в сети интернет» рассматриваются следующие темы.

1. **Основные принципы построения защищенных сетей Интернет**. Классификация уязвимостей OWASP TOP 10. Уязвимости и атаки на веб - приложения. Теоретические основы построения защищенных сетей. Основные элементы многоуровневой системы обеспечения защиты при передаче информации по каналам связи. Классы задач защиты информации в сети. Методы защиты информации в сети интернет. Стратегии защиты информации с использованием современных библиотек ASP.NET.

2. **Аутентификация и авторизация в Интернет**. Протоколы. Методы аутентификации в веб-приложениях. Уязвимости аутентификации. Парольная аутентификация. Аутентификация через Cookie и Session. Авторизация и идентификация. Идентификация и аутентификация с использованием JWT (JSON Web Token). Аутентификация Identity. Identity ASP.NET Core. Авторизация пользователей с помощью ролей. Фильтры авторизации. Анализ защищенности серверных веб - приложений. Безопасность клиентских приложений. Сканеры уязвимостей приложений. Проектирование подсистемы идентификации, аутентификации и авторизации.

3. **Средства и методы интеллектуального обнаружения и предотвращения вторжений**. Архитектура систем обнаружения вторжения. Пассивные и активные системы обнаружения вторжения, системы мониторинга сети (IDS/IPS). Много - агентные системы обнаружения вторжений. Методы машинного обучения для оценки сетевого трафика (линейная регрессия и кластеризация, анализ временных рядов, байесовский классификатор) Использование нейронных сетей для обнаружения сетевых атак. Методы прогнозирования сетевого трафика. Модели программно - конфигурируемых сетей

4. Защита информационных сетей от хакерских атак.Обзор атак, направленных на технологии идентификации, аутентификации и авторизации в системе. Атаки, направленные на выполнении кода. Атаки, направленные на Web-браузеры. Уязвимости, приводящие к выполнению кода.Защита от внедрения операторов SQL Injection.Межсайтовый скриптинг. Межсайтовая подделка HTTP-запросов. Защищенный протокол передачи данных в Интернете. Электронный сертификат.

4. Тематический план

№ п/п	Разделы и темы	Всего часов	Формы занятий			
			лекции	практические занятия	лабораторные занятия	самостоятельная работа
1	Основные принципы построения защищенных сетей Интернет.	18	4	–	4	10
2	Аутентификация и авторизация в Интернет.	18	4	–	4	10
3	Средства и методы интеллектуального обнаружения и предотвращения вторжений	18	4	–	4	10
4	Защита информационных сетей от хакерских атак	18	4	–	4	10
ИТОГО		72	16	–	16	40

5. Виды образовательной деятельности

Занятия лекционного типа

1. **Основные принципы построения защищенных сетей Интернет**. Классификация уязвимостей OWASP TOP 10. Уязвимости и атаки на веб - приложения. Теоретические основы построения защищенных сетей. Основные элементы многоуровневой системы обеспечения защиты при передаче информации по каналам связи. Классы задач защиты информации в сети. Методы защиты информации в сети интернет. Стратегии защиты информации с использованием современных библиотек ASP.NET.

2. А**утентификация и авторизация в Интернет**. Протоколы. Методы аутентификации в веб-приложениях. Уязвимости аутентификации. Парольная аутентификация. Аутентификация через Cookie и Session. Авторизация и идентификация. Идентификация и аутентификация с использованием JWT (JSON Web Token). Аутентификация Identity. Identity ASP.NET Core. Авторизация пользователей с помощью ролей. Фильтры авторизации. Анализ защищенности серверных веб - приложений. Безопасность клиентских приложений. Сканеры уязвимостей приложений. Проектирование подсистемы идентификации, аутентификации и авторизации.

3. **Средства и методы интеллектуального обнаружения и предотвращения вторжений**. Архитектура систем обнаружения вторжения. Пассивные и активные системы обнаружения вторжения, системы мониторинга сети (IDS/IPS). Много - агентные системы обнаружения вторжений. Методы машинного обучения для оценки сетевого трафика (линейная регрессия и кластеризация, анализ временных рядов, байесовский классификатор) Использование нейронных сетей для обнаружения сетевых атак. Методы прогнозирования сетевого трафика. Модели программно - конфигурируемых сетей

4. Защита информационных сетей от хакерских атак.Обзор атак, направленных на технологии идентификации, аутентификации и авторизации в системе. Атаки, направленные на выполнении кода. Атаки, направленные на Web-браузеры. Уязвимости, приводящие к выполнению кода.Защита от внедрения операторов SQL Injection.Межсайтовый скриптинг. Межсайтовая подделка HTTP-запросов. Защищенный протокол передачи данных в Интернете. Электронный сертификат.

Занятия семинарского типа

Не предусмотрены

Лабораторные работы

ЛБ 1. Аутентификация веб-приложений ASP.NET Core MVC на основе токенов.
ЛБ 2. Аутентификация веб-приложений ASP.NET Core MVC Identity.
ЛБ 3. Авторизация в ASP.NET Core Web API с помощью токенов.
ЛБ 4. Авторизация средствами ASP.NET Core Identity.
ЛБ 5. Валидация данных в веб - приложениях.
ЛБ 6. Веб-приложение, уязвимое для SQL-инъекций.
ЛБ 7. Разработка веб-приложений, уязвимых для XSS-атак.
ЛБ 8. Веб-приложения, уязвимые для CSRF-атак.

Задания для лабораторных работ, размещены в системе дистанционного обучения СмолГУ (www.moodle.smolgu.ru). На занятиях для каждой работы задание предоставляется студентам в электронном виде.

Самостоятельная работа

Текущая самостоятельная работа студента направлена на углубление и закрепление знаний студентов, развитие практических умений. Она заключается в работе с лекционными материалами, поиске и обзоре литературы и электронных источников, информации по заданным темам курса, опережающей самостоятельной работе, в изучении тем, вынесенных на самостоятельную проработку, подготовке к лабораторным занятиям.

Самостоятельная внеаудиторная работа студентов включает:

- проработку лекционного материала, составление конспекта лекций по темам, вынесенным на самостоятельное изучение;
- выполнение домашних заданий;
- подготовку к защите лабораторных работ.

Темы для самостоятельного изучения

1. Атаки, направленные на технологии идентификации и аутентификации.
2. Атаки, направленные на выполнении кода.
3. .Атаки, направленные на Web-браузеры.
4. Атаки, направленные на разглашение информации.
5. Логические атаки.

Учебно-методическое обеспечение для самостоятельной работы

1. Лаврищева, Е. М. Программная инженерия и технологии программирования сложных систем : учебник для вузов / Е. М. Лаврищева. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 432 с. — (Высшее образование). — ISBN 978-5-534-07604-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/470923

6. Критерии оценивания результатов освоения дисциплины (модуля)

6.1. Оценочные средства и критерии оценивания для текущей аттестации

Теоретические вопросы

1. Основные принципы построения защищенных сетей Интернет. Классификация уязвимостей OWASP TOP 10. Уязвимости и атаки на веб - приложения.
2. Теоретические основы построения защищенных сетей. Основные элементы многоуровневой системы обеспечения защиты при передаче информации по каналам связи.
3. Классы задач защиты информации в сети. Методы защиты информации в сети интернет.
4. Стратегии защиты информации с использованием современных библиотек ASP.NET.
5. Аутентификация и авторизация в Интернет. Протоколы.
6. Методы аутентификации в веб-приложениях. Уязвимости аутентификации. Парольная аутентификация. Аутентификация через Cookie и Session.
7. Авторизация и идентификация. Идентификация и аутентификация с использованием JWT (JSON Web Token). Аутентификация Identity. Identity ASP.NET Core.
8. Авторизация пользователей с помощью ролей. Фильтры авторизации.
9. Анализ защищенности серверных веб - приложений.
10. Безопасность клиентских приложений. Сканеры уязвимостей приложений.
11. Проектирование подсистемы идентификации, аутентификации и авторизации.
12. Средства и методы интеллектуального обнаружения и предотвращения вторжений. Архитектура систем обнаружения вторжения.
13. Пассивные и активные системы обнаружения вторжения, системы мониторинга сети (IDS/IPS). Много-агентные системы обнаружения вторжений.
14. Методы машинного обучения для оценки сетевого трафика (линейная регрессия и кластеризация, анализ временных рядов, байесовский классификатор) Использование нейронных сетей для обнаружения сетевых атак.
15. Методы прогнозирования сетевого трафика. Модели программно - конфигурируемых сетей
16. Защита информационных сетей от хакерских атак.Обзор атак, направленных на технологии идентификации, аутентификации и авторизации в системе.
17. Атаки, направленные на выполнении кода. Атаки, направленные на Web-браузеры.

18. Уязвимости, приводящие к выполнению кода.Защита от внедрения операторов SQL Injection.
19. Межсайтовый скриптинг. Межсайтовая подделка HTTP-запросов.
20. Защищенный протокол передачи данных в Интернете. Электронный сертификат.

Критерии оценивания теоретических вопросов

1. Нормы оценивания ответов на теоретические вопросы

№ п/п	Теоретический вопрос	Количество баллов (*)
1	Дан краткий ответ на поставленный вопрос	1 балл
2	Дан развернутый ответ на вопрос с анализом результатов	2 балла

(*) Возможна градация в 0,25 балла.

2. Шкала оценивания. Оценка «зачтено» за ответы на теоретические вопросы выставляется, если набрано не менее 3 баллов при ответе на три вопроса, в противном случае выставляется «не зачтено».

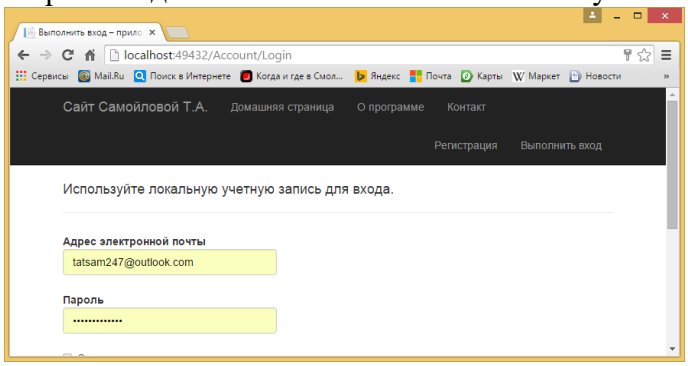
Задания для лабораторных занятий

Задачи по темам курса предложены к каждому лабораторному занятию.

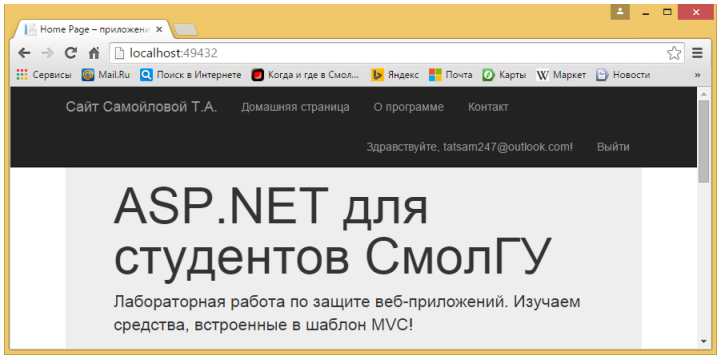
Образцы заданий

Задание 1.Создайте MVC - проект, включающий готовую систему аутентификации и авторизации ASP.NET Identity. Испытайте ее и посмотрите результаты испытаний в базе данных. Далее представлены примерные формы, которые должны быть созданы в результате отладки проекта:

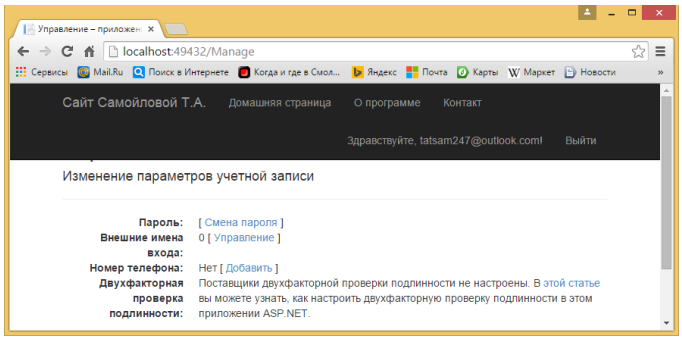
Форма входа с использованием локальной учетной записи:

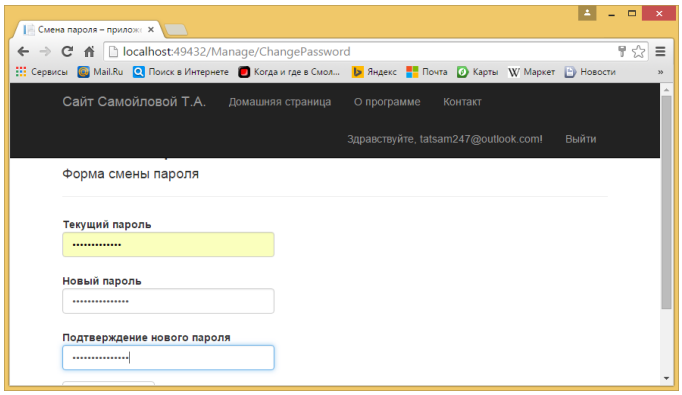


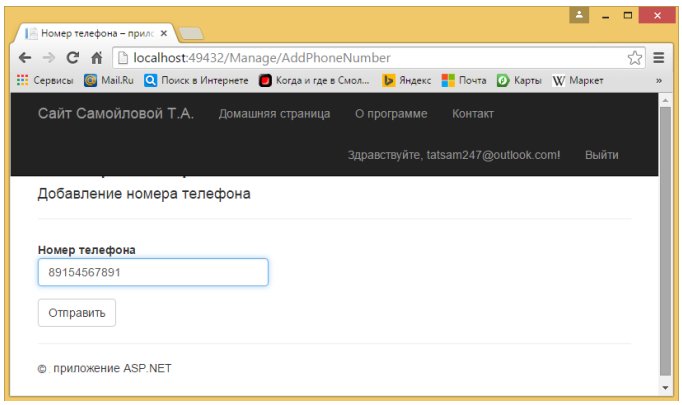
Форма приветствия (после регистрации):

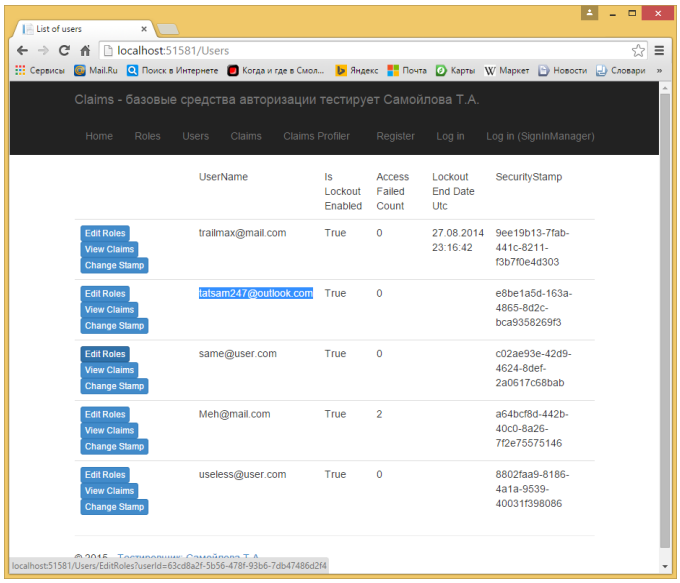


Изменение параметров учетной записи:









Задание 2. Создайте MVC - веб-приложение в среде **ASP.NETCore**для выполнения операции SELECT над таблицей пользователей (Users), содержащей информацию о вкладах. В названии проекта – ваша фамилия. Организуйте вывод вклада по введенному паролю

пользователя. При вводе вместе в паролем «инъекции» - выводится вся таблица паролей и вкладов.

Критерии оценивания выполнения лабораторных работ

1. Нормы оценивания каждой лабораторной работы:

№п/п	Структурная часть работы	Количество баллов (*)
1	Ответ на теоретические вопросы по теме лабораторной работы	1 балл
2	Демонстрация выполнения конкретного задания, предложенного для самостоятельного решения к лабораторной работе	2 балла

(*) с возможностью градации до 0,25 балла.

2. Шкала оценивания. Оценка «зачтено» за лабораторную работу выставляется, если набрано не менее 2 баллов, в противном случае за работу выставляется «не зачтено».

6.2. Оценочные средства и критерии оценивания для промежуточной аттестации

Зачетная контрольная работа

1. В ваш готовый веб – проект добавьте систему авторизации для «авторского» входа на страницы. На каждую из страниц разрешите вход только конкретным пользователям. Испытайте проект для разных пользователей.
2. Разработайте два сайта: уязвимый и атакующий. Уязвимый сайт принимает от клиента простую отправку формы. Посредством него вы отправляете в течение дня запросы - перевод средств между банковскими счетами, покупки или продажи ценных бумаг, увеличение кредита и так далее. Атакующий сайт хакера формирует специальный запрос от вашего имени, для этого он посылает вам страницу, которая создает с вашего компьютера вредоносный запрос к уязвимому приложению.

Критерии оценивания зачетной контрольной работы

1. Нормы оценивания работы

№ п/п	Структурная часть контрольной работы	Количество баллов (*)
1	Правильно реализован каждый метод решения	1 балл
2	Анализ результатов	2 балла

(*) Возможна градация в 0,25 балла.

2. Шкала оценивания работы:

п/п	Оценка	Количество баллов
1	Отлично	4,75-5
2	Хорошо	3,75-4,5
3	Удовлетворительно	3-3,5
4	Неудовлетворительно	менее 3

Критерий получения зачета

Зачет выставляется по результатам работы студента в течение семестра согласно Положению о текущем контроле успеваемости и промежуточной аттестации обучающихся в федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Смоленский государственный университет» (утверждено приказом ректора № 01-113 от 26.09.2019 г.; внесены дополнения приказом ректора № 01-48 от 30.04.2020).

Для получения зачета студент должен:

- уметь отвечать на теоретические вопросы, рассмотренные на лекциях;
- уметь решать задачи, предложенные на лабораторных занятиях;

- уметь решать задачи, предложенные на зачетной контрольной работе.

7. Перечень основной и дополнительной учебной литературы

7.1. Основная литература

1. Васильева И.Н.Криптографические методы защиты информации: учебник и практикум для вузов/ И.Н.Васильева.— Москва: Издательство Юрайт, 2020.— 349с.— (Высшее образование).— ISBN978-5-534-02883-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL:https://urait.ru/bcode/450998.
2. Внуков А.А.Защита информации: учебное пособие для вузов/ А.А.Внуков.— 3-е изд., перераб. и доп.— Москва: Издательство Юрайт, 2020.— 161с.— (Высшее образование).— ISBN978-5-534-07248-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL:https://urait.ru/bcode/422772(дата обращения: 07.05.2021).
3. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2021. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/470351

7.2. Дополнительная литература

1. Бабенко Л.К.Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов/ Л.К.Бабенко, Е.А.Ищукова.— Москва: Издательство Юрайт, 2020.— 220с.— (Высшее образование).— ISBN978-5-9916-9244-1. — Текст: электронный // ЭБС Юрайт [сайт]. — URL:https://urait.ru/bcode/452871.
2. Внуков А.А.Защита информации в банковских системах: учебное пособие для вузов/ А.А.Внуков.— 2-е изд., испр. и доп.— Москва: Издательство Юрайт, 2020.— 246с.— (Высшее образование).— ISBN978-5-534-01679-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL:https://urait.ru/bcode/468273.

7.3.Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Система дистанционного обучения СмолГУ (moodle.smolgu.ru).
2. Интернет-Университет Информационных Технологий, лекции:Обеспечение безопасности веб - приложений, учебный курс, https://intuit.ru/studies/courses/2336/636/lecture/13823

8. Материально-техническое обеспечение

Для занятий необходимы:

1. проектор;
2. интерактивная доска;
3. персональные компьютеры.

Для самостоятельной работы подготовлены аудитории № 224, 226, 230, 234 с выходом в Интернет, оснащенные компьютерами IBMPCс процессорами IntelCore 7 и оперативной памятью не менее 16 ГБ.

9.Программное обеспечение

1. MICROSOFT VISUAL STUDIO COMMUNITY 2019
2. СУБД SQLServer EXPRESS 2019