


МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Чувашский государственный университет имени И. Н. Ульянова»

Факультет информатики и вычислительной техники

Кафедра математического и аппаратного обеспечения информационных систем

«УТВЕРЖДАЮ»

Проректор по учебной работе


И.Е. Поверинов

31 августа 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Виртуальные частные сети»

Специальность – 10.05.03 «Информационная безопасность автоматизированных систем»

Квалификация (степень) выпускника – Специалист по защите информации

Специализация – «Безопасность открытых информационных систем»

Рабочая программа основана на требованиях Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом Министерства образования и науки №1509 от 01.12.2016 г.

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

Доцент, к.ф.-м.н.
старший преподаватель

 Д.В.Ильин
С.О. Иванов

ОБСУЖДЕНО:


на заседании кафедры математического и аппаратного
обеспечения информационных систем
«30» августа 2017г., протокол №1

заведующий кафедрой
СОГЛАСОВАНО:

 Д.В. Ильин

Методическая комиссия факультета информатики и вычислительной техники
«30» августа 2017г., протокол №1

Декан факультета

 А.В. Щипцова

Директор научной библиотеки

 Н.Д. Никитина

Начальник управления информатизации

 И.П. Пивоваров

Начальник учебно-методического управления

 В.И. Маколов

Оглавление

1. Цель и задачи обучения по дисциплине	4
2. Место дисциплины в структуре основной образовательной программы (ООП)	4
3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП.....	4
4. Структура и содержание дисциплины.....	5
4.1. Содержание дисциплины	5
4.2. Объем дисциплины, виды учебной работы обучающихся по очной форме обучения.....	5
5. Содержание разделов дисциплины	5
5.1. Лекции и практические занятия.....	5
5.2. Лабораторные работы	6
5.3. Вопросы для самостоятельной работы студента	7
6. Образовательные технологии.....	7
7. Формы аттестации и оценочные материалы.....	8
7.1. Вопросы к экзамену.....	8
7.2. Оценивание результатов экзамена	9
8. Учебно-методическое и информационное обеспечение дисциплины	9
8.1. Рекомендуемая основная литература	9
8.2. Рекомендуемая дополнительная литература.....	9
8.3. Программное обеспечение, профессиональные базы данных, информационно-справочные системы.	10
8.4. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.....	10
9. Материально-техническое обеспечение дисциплины.....	10
10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями.....	11
11. Методические рекомендации по освоению дисциплины.....	11

1. Цель и задачи обучения по дисциплине

Цель дисциплины: получение навыков применения технологий виртуальных частных сетей для защиты сетевых соединений.

Основными задачами дисциплины являются:

- выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;
- реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем.

2. Место дисциплины в структуре основной образовательной программы (ООП)

Дисциплина «Виртуальные частные сети» относится к числу дисциплин базовой части профессионального цикла. Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: «Основы информационной безопасности», «Безопасность операционных систем», «Безопасность сетей ЭВМ».

Дисциплина является предшествующей для прохождения практик, государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП

Процесс обучения по дисциплине направлен на формирование следующих компетенций:

- способность к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8);
- способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);
- способность формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем (ПСК-4.5).

В результате обучения по дисциплине, обучающийся должен (ЗУН):

знать:

- технологии и методы защиты сетевых соединений (31);
- принципы построения виртуальных сетей, защищенных соединений и виртуальных частных сетей (32);
- принципы и технологии защиты сетевого трафика (33);

уметь:

- обеспечивать и контролировать защиту сетевых соединений (У1);
- применять знания для проектирования, создания и контроля виртуальных частных сетей (У2);
- организовывать инфраструктуру для обеспечения работы виртуальных сетей (У3);

владеть:

- средствами защиты сетей и вспомогательными средствами (Н1);
- протоколами, стандартами и специальным программным обеспечением, используемым в области виртуальных частных сетей (Н2);

- утилитами и инструментальными средствами по созданию виртуальных сетей (НЗ).

4. Структура и содержание дисциплины

Образовательная деятельность по дисциплине проводится:

- в форме контактной работы обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (далее – контактная работа);
- в форме самостоятельной работы.

Контактная работа включает в себя занятия лекционного типа, занятия семинарского типа (семинары, практические занятия, лабораторные работы, практикумы), групповые и (или) индивидуальные консультации, в том числе в электронной информационно-образовательной среде.

Обозначения:

Л – лекции, л/р – лабораторные работы, п/р – практические занятия, КСР – контроль самостоятельной работы, СРС – самостоятельная работа студента, ИФР – интерактивная форма работы, К – контроль.

4.1. Содержание дисциплины

Содержание	Формируемые компетенции	Формируемые ЗУН
Раздел 1. Основы VPN.	ОПК-8	32, У2, Н2
Тема 1.1. Эволюция виртуальных частных сетей.		
Тема 1.2. Архитектура VPN.		
Раздел 2. Защита сетевых соединений.	ПК-24, ПСК-4.5	32-33, У2-У3, Н2-Н3
Тема 2.1 Технологии защиты сетевых соединений.		
Тема 2.2. Технологии контроля сетевых соединений.		
Экзамен	ОПК-8, ПК-24, ПСК-4.5	31, 32, У1, Н2

4.2. Объем дисциплины, виды учебной работы обучающихся по очной форме обучения

Содержание	Всего, час	Контактная работа, час				СРС, час	ИФР, час	К, час
		Л	л/р	п/р	КСР			
Раздел 1. Основы VPN.								
Тема 1.1. Эволюция виртуальных частных сетей.	22	4	4	6		8	2	
Тема 1.2. Архитектура VPN.	40	6	6	12		16	2	
Раздел 2. Защита сетевых соединений.								
Тема 2.1 Технологии защиты сетевых соединений.	23	2	2	8		11	2	
Тема 2.2. Технологии контроля сетевых соединений.	21	4	4	6		7	2	
Экзамен	38				2			36
Итого	144 4 з.е.	16	16	32	2	42	8	36

5. Содержание разделов дисциплины

5.1. Лекции и практические занятия

Раздел 1. Основы VPN.

Тема 1.1. Эволюция виртуальных частных сетей.

Лекция 1. Понятие виртуальных частных сетей.

1. Характеристики VPN.
2. Применение VPN.
3. Достоинства и недостатки VPN.

Практическое занятие 1. Session Traversal Utilities for NAT (STUN)

Лекция 2. Сертификаты.

1. Структура и форматы сертификата.
2. Получение и генерация сертификата.
3. Проверка цепочки сертификатов.

Практическое занятие 2. Генерация цифровых сертификатов.

Практическое занятие 3. Проверка сертификатов.

Тема 1.2. Архитектура VPN.

Лекция 3. Структура VPN.

1. Классификация средств VPN.
2. Основные алгоритмы и протоколы.

Практическое занятие 4. Протокол PPPoE.

Лекция 4. Топология VPN.

1. Виды топологий.
2. Принципы организации и особенности работы топологий.

Практическое занятие 5. Безопасность на основе IEEE 802.1x.

Лекция 5. Протоколы VPN.

1. Протоколы аутентификации.
3. Протоколы шифрования.
2. Протоколы туннелирования и коммутации.

Практическое занятие 6. Туннелирование и шифрование соединений.

Практическое занятие 7. Опportunистическое шифрование трафика Терсгрут

Раздел 2. Защита сетевых соединений.

Тема 2.1 Технологии защиты сетевых соединений.

Лекция 6. OpenVPN.

1. Архитектура OpenVPN.
2. Настройка сервера OpenVPN.
3. Настройка клиента OpenVPN.

Практическое занятие 9. Клиент-серверные виртуальные частные сети.

Практическое занятие 10. Клиент-сетевые виртуальные частные сети.

Тема 2.2. Технологии контроля сетевых соединений.

Лекция 7. Виртуальные локальные сети.

1. Назначение виртуальных локальных сетей.
2. Стандарт IEEE 802.1q.
3. Настройка виртуальной локальной сети в ОС.

Практическое занятие 11. Виртуальные локальные сети IEEE 802.1q.

Лекция 8. HTTP-проxy и SOCKS.

1. Назначение и принцип работы прокси.
2. Фильтрация трафика.
3. Принцип работы SOCKS.

Практическое занятие 12. Технология фильтрации IP-MAC Binding.

5.2. Лабораторные работы

Тема	Количество часов
Лабораторная работа 1. STUNTMAN.	2
Лабораторная работа 2. OpenSSL.	2
Лабораторная работа 3. Rp-pppoe.	2
Лабораторная работа 4. Freeradius.	2
Лабораторная работа 5. Stunnel.	2
Лабораторная работа 6. OpenVPN	2
Лабораторная работа 7. VLAN.	2
Лабораторная работа 8. Privoxy.	2

Итого	16
--------------	----

5.3. Вопросы для самостоятельной работы студента

Раздел 1. Основы VPN.

1. Стандарт IEEE 802.1x.
2. Аудит безопасности протокола IPSec.
3. Аудит безопасности протокола PPTP, L2TP.
4. Аудит безопасности протокола TLS.
5. Аудит безопасности протокола PAP/CHAP.

Раздел 2. Защита сетевых соединений

1. Аудит безопасности протокола SNMP.
2. Шифрование канала с использованием протокола WEP.
3. Шифрование канала с использованием протоколов WPA, WPA-2.
4. Аутентификация беспроводных клиентов на основе учётных записей пользователей и аппаратных адресов компьютеров.
5. Система обнаружения вторжений snort.
6. Настройка аппаратного межсетевого экрана
7. Система контроля трафика;
8. Безопасность индивидуального порта;
9. Ограничение количества управляющих коммутатором узлов сети.
10. Безопасность на основе технологии сегментации трафика.
11. Списки контроля доступа ACL.
12. Контроль доступа к коммутатору.

6. Образовательные технологии

В соответствии со структурой образовательного процесса по дисциплине применяются следующие технологии:

- применения знаний на практике, поиска новой учебной информации;
- организации совместной и самостоятельной деятельности обучающихся (учебно-познавательной, научно-исследовательской, частично-поисковой, репродуктивной, творческой и пр.).

В соответствии с требованиями ФГОС ВО для реализации компетентного подхода при обучении дисциплине предусмотрено широкое использование в учебном процессе активных и интерактивных методов проведения занятий:

При обучении дисциплине применяются следующие формы занятий:

- лекции, направленные на получение новых и углубление научно-теоретических знаний, в том числе вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция, лекции-дискуссии, лекции-беседы и др.;
- практические занятия, проводимые под руководством преподавателя в учебной аудитории, направленные на углубление и овладение определенными методами самостоятельной работы, могут включать коллективное обсуждение материала, дискуссии, решение и разбор конкретных практических ситуаций, компьютерные симуляции, тренинги и др.;
- лабораторные занятия, проводимые под руководством преподавателя в учебной лаборатории с использованием компьютеров и учебного оборудования, направленные на закрепление и получение новых умений и навыков, применение знаний и умений, полученных на теоретических занятиях, при решении практических задач и др.

Все занятия обеспечены мультимедийными средствами (SMART доски, проекторы, экраны) для повышения качества восприятия изучаемого материала. В образовательном процессе широко используются информационно-коммуникационные технологии.

Самостоятельная работа студентов – это планируемая работа студентов, выполняемая по заданию при методическом руководстве преподавателя, но без его непосредственного участия. Формы самостоятельной работы студентов определяются содержанием учебной дисциплины, степенью подготовленности студентов. Они могут иметь учебный или учебно-исследовательский характер: анализ, аннотирование и конспектирование литературы по теме, составление вопросов и тестов к теме, подготовка к лабораторным работам, подготовка реферативных сообщений.

Формами контроля самостоятельной работы выступают оценивание устного выступления студента на практическом занятии, его доклада; проверка письменных отчётов по результатам выполненных заданий и лабораторных работ. Результаты самостоятельной работы учитываются при оценке знаний на экзамене.

7. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме экзамена. Принимается экзамен преподавателем, читающим лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний обучающихся.

7.1. Вопросы к экзамену

1. Чем отличаются различные реализации VPN?
2. Опишите для чего применяются виртуальные частные сети.
3. Какие есть альтернативные технологии VPN?
4. Приведите примеры реализации VPN.
5. Что такое цифровой сертификат?
6. Что такое CSR-запрос?
7. Где находятся ключи сертификата?
8. Опишите способы проверки сертификата.
9. Какие существуют виды VPN по реализации и уровням?
10. Как происходит шифрование трафика в VPN?
11. Перечислите технологии для туннелирования трафика VPN.
12. Перечислите технологии для коммутации трафика VPN.
13. Опишите принцип работы и настройки клиент-серверной VPN.
14. Опишите принцип работы и настройки клиент-сетевой VPN.
15. Опишите принцип работы и настройки межсетевой VPN.
16. Опишите принцип работы и настройки выделенной VPN.
17. Перечислите и опишите протоколы аутентификации.
18. Перечислите и опишите протоколы шифрования.
19. Перечислите и опишите протоколы туннелирования.
20. Перечислите и опишите протоколы коммутации.
21. Чем проксирование трафика отличается от форвардинга?
22. Какие существуют прокси-сервера?
23. Как происходит фильтрация трафика прокси-сервером?
24. Почему SOCKS быстрее и безопаснее прокси уровня приложений.
25. Какие существуют варианты реализации виртуальных сетей?
26. Чем VLAN отличается от VPN?
27. Опишите принцип работы виртуальной сети по IEEE 802.1q.
28. Как подключиться к виртуальной частной сети?
29. Опишите преимущества и недостатки OpenVPN.

30. Как создаются сертификаты для OpenVPN?
31. Чем отличаются tun и tap режимы работы OpenVPN?
32. Какие сетевые порты необходимы для работы OpenVPN?

7.2. Оценивание результатов экзамена

Экзаменационный билет для проведения промежуточной аттестации включают вопросы и задачи для проверки сформированности знаний, умений и навыков.

Общими критериями, определяющими оценку знаний, умений и навыков на экзамене, являются:

для оценки «отлично» - наличие глубоких и исчерпывающих знаний в объёме пройденного программного материала правильные и уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, знание дополнительно рекомендованной литературы;

для оценки «хорошо» - наличие твердых и достаточно полных знаний программного материала, незначительные ошибки при освещении заданных вопросов, правильны действия по применению знаний на практике, четкое изложение материала;

для оценки «удовлетворительно» - наличие твердых знаний пройденного материала, изложение ответов с ошибками, уверенно исправляемыми после дополнительных вопросов, необходимость наводящих вопросов, правильные действия по применению знаний на практике;

для оценки «неудовлетворительно» - наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

8. Учебно-методическое и информационное обеспечение дисциплины

Электронный каталог и электронные информационные ресурсы, предоставляемые научной библиотекой ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке <http://library.chvsu.ru/>

8.1. Рекомендуемая основная литература

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Васин Н.Н. Построение сетей на базе коммутаторов и маршрутизаторов [Электронный ресурс] / Н.Н. Васин. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 330 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52162.html
2.	Криптография и безопасность цифровых систем [Электронный ресурс] : учебное пособие / В.Г. Грибунин [и др.]. — Электрон. текстовые данные. — Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2011. — 411 с. — 978-5-9515-0166-0. — Режим доступа: http://www.iprbookshop.ru/60851.html

8.2. Рекомендуемая дополнительная литература

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Алексеев В.А. Маршрутизация и защита сетевого трафика в сетях TCP/IP [Электронный ресурс] : методические указания к проведению лабораторных работ по курсу «Сетевые технологии» / В.А. Алексеев. — Электрон. текстовые данные. — Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2013. — 35 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/55104.html
2.	Оливер Ибе Компьютерные сети и службы удаленного доступа [Электронный ресурс] : учебное пособие / Ибе Оливер. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 333 с. Режим доступа: http://www.iprbookshop.ru/63577.html

8.3. Программное обеспечение, профессиональные базы данных, информационно-справочные системы.

Программное обеспечение, профессиональные базы данных, информационно-справочные системы, предоставляемые управлением информатизации ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке <http://ui.chuvsu.ru/>*

8.3.1 Программное обеспечение

№ п/п	Наименование	Условия доступа/скачивания
1.	MS Windows/CentOS	лицензия университета/ свободное лицензионное соглашение (https://www.centos.org/download/)
2.	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
3.	Виртуальная машина Virtualbox	свободное лицензионное соглашение на ПО: GNU GPL (https://www.virtualbox.org/wiki/Downloads)
4.	ПО для создания виртуальной частной сети	Свободное лицензионное соглашение на ПО: GNU GPL (https://openvpn.net/index.php/download/community-downloads.html)

8.3.2 Базы данных, информационно-справочные системы

№ п/п	Наименование программного обеспечения	Условия доступа/скачивания
1.	Гарант	из внутренней сети университета (договор)*
2.	Консультант +	

8.4. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.

№ п/п	Наименование	Условия доступа
1.	Xgu.ru.	http://xgu.ru/wiki/
2.	Российская Государственная Библиотека	http://www.rsl.ru
3.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
4.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
5.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
6.	Научная электронная библиотека	http://elibrary.ru
7.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
8.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru

9. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине оснащены автоматизированным рабочим местом (АРМ) преподавателя, обеспечивающим тематические иллюстрации и демонстрации, соответствующие программе дисциплины в составе:

- ПЭВМ с доступом в интернет (операционная система, офисные программы, антивирусные программы);
- мультимедийный проектор с дистанционным управлением;

Учебные аудитории для практических, лабораторных и самостоятельных занятий по дисциплине оснащены АРМ преподавателя и пользовательскими АРМ по числу обучающихся, объединенных локальной сетью («компьютерный» класс), с возможностью

подключения к сети Интернет и доступом к электронной информационно-образовательной среде ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова», структурированная кабельная система (кабели UTP5, коннекторы 8p8c, инструменты для создания и тестирования патчкордов); телекоммуникационное оборудование (коммутаторы, WiFi-роутеры); программно-аппаратные комплексы защиты информации (АПКШ «Континент» Платформа IPC-25).

10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

11. Методические рекомендации по освоению дисциплины

В ходе лекционных занятий студенту рекомендуется вести конспектирование учебного материала. Следует обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. При составлении конспекта желательно оставлять в рабочих конспектах поля, на которых в дальнейшем можно делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. В ходе лекционных занятий рекомендуется задавать преподавателю уточняющие вопросы с целью выяснения теоретических положений, разрешения спорных ситуаций.

В ходе подготовки к практическим занятиям и лабораторным работам рекомендуется изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях. основой для выполнения лабораторной работы являются разработанные кафедрой методические указания. Рекомендуется дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой дисциплины. Желательно подготовить тезисы для выступлений по всем учебным вопросам, выносимым на практическое занятие. Готовясь к докладу или реферативному сообщению, рекомендуется обращаться за методической помощью к преподавателю, составить план-конспект своего выступления, продумать примеры с целью обеспечения тесной связи изучаемой теории с практикой. В процессе подготовки студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании выпускной квалификационной работы.

Формы организации студентов на лабораторных работах и практических занятиях: групповая. При групповой форме организации занятий одна и та же работа выполняется бригадами по 2 - 5 человек.

Если в результате выполнения лабораторной работы запланирована подготовка письменного отчета, то отчет о выполненной работе необходимо оформлять в соответствии с требованиями методических указаний. Качество выполнения лабораторных работ является важной составляющей оценки текущей успеваемости обучающегося.