Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой ИБСиТ
_____ В.Ф. Антонов
«____» _____ 202_ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущей и промежуточной аттестации

По дисциплине	Б1.Б.29 «Криптографические методы защиты информации»	
Направление подготовки	10.03.01 Информационная безопасность	
Направленность (профиль)	Комплексная защита объектов информатизации	
Квалификация выпускника	бакалавр	
Форма обучения	очная	
Учебный план	2020 г.	
Объем занятий: Итого	135,0 ч.	5 з.е.
В т.ч. аудиторных	76,5 ч.	
Из них:		
Лекций	25,5 ч.	
Лабораторных работ	51,0 ч.	
Практических занятий	___ ч.	
Самостоятельной работы	31,5 ч.	
Зачет в 5 семестре	___ ч.	
Экзамен в 6 семестре	27,0 ч.	

Дата разработки:

Предисловие

1. Фонд оценочных средств предназначен для проверки знаний, умений и навыков при проведении текущего и промежуточного контроля.

2. Фонд оценочных средств текущего контроля и промежуточной аттестации на основе рабочей программы дисциплины, составлен в соответствии с образовательной программой по направлению подготовки 10.03.01 Информационная безопасность, утвержденной на заседании учебно-методического совета ФГАОУ ВО «СКФУ» протокол № 1 от «29» сентября 2020 г.

3. Разработчик _____ Битюцкая Н.И.., доцент кафедры ИБСиТ

4. ФОС рассмотрен и утвержден на заседании кафедры информационной безопасности, систем и технологий Протокол № 2 от «4» сентября 2020г.

5. ФОС согласован с выпускающей кафедрой кафедры информационной безопасности, систем и технологий Протокол № 2 от «4» сентября 2020г.

6. Проведена экспертиза ФОС. Члены экспертной группы, проводившие внутреннюю экспертизу:
Председатель_____ Антонов В.Ф.
_____ Мишин В.В.
_____ Сорокин И.Д.

Экспертное заключение: данные оценочные средства соответствует требованиям федерального государственного образовательного стандарта высшего образования, рекомендуются для использования в учебном процессе.
«____»_____

_____(подпись)

7. Срок действия ФОС один год.

Паспорт фонда оценочных средств
для проведения текущей и промежуточной аттестации

По дисциплине	Б1.Б.29 «Криптографические методы защиты информации»
Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль)	Комплексная защита объектов информатизации
Квалификация выпускника	бакалавр
Форма обучения	очная
Учебный план	2020 г.

Код оцениваемой компетенции (или её части)	Модуль, раздел, тема (в соответствии с Программой)	Тип контроля	Вид контроля	Компонент фонда оценочных средств	Количество заданий для каждого уровня, шт.	
					Базовый	Повышенный
5 семестр						
ОПК-2, ОПК-4, ПК-1	Темы 1 - 9	текущий	устный	Вопросы для собеседования	13	9
	Темы 1 – 4, 6	текущий	письменный	Темы индивидуальных заданий для лабораторных работ	8	4
6 семестр						
ОПК-2, ОПК-4, ПК-1	Темы 10 - 17	текущий	устный	Вопросы для собеседования	22	7
ОПК-2, ОПК-4, ПК-1	Темы 10,12, 14 - 16	текущий	письменный	Темы индивидуальных заданий для лабораторных работ	4	2
ОПК-2, ОПК-4, ПК-1	Темы 1 - 17	промежуточный	устный	Вопросы к экзамену	29	19
			устный	Вопросы для проверки уровня знаний	19	14
			устный	Вопросы (задания) для проверки умений и навыков	10	5

Составитель _____ Битюцкая Н.И.
(подпись)

«____»_____20 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой ИБСиТ

_____ В.Ф. Антонов

«____» _____ 202_ г.

Вопросы для собеседования

по дисциплине Криптографические методы защиты информации»

5 семестр

Базовый уровень

Тема 1. Основные понятия криптографии.

1. Основные понятия криптографии.

Тема 2. Классические шифры замены.

2. Наиболее известные классические шифры замены.

Тема 3. Классические шифры перестановки.

3. Наиболее известные классические шифры перестановки.

Тема 4. Современные блочные шифры с симметричным ключом.

4. Принципы построения современных блочных шифров с симметричным ключом.
5. Основные компоненты современного блочного шифра.
6. Шифры Фейстеля и не-Фейстеля.

Тема 5. Современные поточные шифры с симметричным ключом.

7. Принципы построения современных поточных шифров с симметричным ключом. Синхронные и несинхронные шифры потока.
8. Преимущества и проблемы современных шифров потока.

Тема 6. Современный стандарт шифрования (DES)

9. Современный стандарт шифрования (DES). Структура шифра DES. Раунды шифрования. Функция DES. Генерация ключей раундов.

Тема 7. Усовершенствованный стандарт шифрования (AES).

10. Алгоритм расширения ключей. Анализ расширения ключа. Алгоритмы шифрования и дешифрования в AES.

Тема 8. Российский стандарт ГОСТ 28147-89.

11. Алгоритмы шифрования и дешифрования в российском стандарте ГОСТ 28147-89.

Тема 9. Алгоритмы шифрования с открытыми ключами.

12. Концепция криптографии с открытым ключом.
13. Криптосистема RSA.

Повышенный уровень

Тема 1. Основные понятия криптографии.

1. Виды атак криптоанализа. Способы противодействия им.

Тема 2. Классические шифры замены.

2. Криптоанализ шифров замены.

Тема 3. Классические шифры перестановки.

3. Криптоанализ шифров перестановки.
Тема 4. Современные блочные шифры с симметричным ключом.
4. Атаки на блочные шифры.
Тема 5. Современные поточные шифры с симметричным ключом.
5. Криптоанализ шифров потока.
Тема 6. Современный стандарт шифрования (DES)
6. Двукратный и трехкратный DES.
7. Криптоанализ шифра DES.
Тема 7. Усовершенствованный стандарт шифрования (AES).
8. Анализ AES.
Тема 9. Алгоритмы шифрования с открытыми ключами.
9. Стойкость RSA. Виды атак на RSA.

6 семестр

Базовый уровень

Тема 10. Алгоритмы генерации простых чисел. Проверка чисел на простоту.
1. Алгоритмы генерации простых чисел.
2. Способы проверки на простое число. Решето Эратосфена.
3. Phi-функция Эйлера. Простые числа Мерсенны. Простые числа Ферма.
4. Детерминированные и вероятностные алгоритмы проверки чисел на простоту.
Тема 11. Сложность криптографических алгоритмов.
5. Понятие и оценка сложности криптографических алгоритмов.
Тема 12. Криптосистемы с открытым ключом.
6. Криптосистема Рабина.
7. Криптографическая система Эль-Гамаля.
8. Алгоритмы шифрования, дешифрования и генерации ключей в криптосистемах Рабина и Эль-Гамаля.
Тема 14. Аутентификация данных. Электронная цифровая подпись.
9. Понятие электронной цифровой подписи и требования к ней.
10. Алгоритмы ЭЦП: RSA, Эль-Гамаля.
11. Алгоритмы ЭЦП: ФиатаШамира, Онга-Шнорра-Шамира.
12. Неотрицаемая подпись Шаума-ванАнтверпена.
Тема 15. Генерация и проверка цифровой подписи на основе криптосистемы Эль-Гамаля.
13. Генерация и проверка цифровой подписи на основе криптосистемы Эль-Гамаля.
Тема 16. Понятие о структуре и способах построения криптографических протоколов.
14. Понятие криптографического протокола. Основные примеры.
15. Связь стойкости протокола со стойкостью базовой криптографической системы.
16. Классификация криптографических протоколов.
17. Парольные схемы и протоколы "рукопожатия".
18. Взаимосвязь между протоколами аутентификации и цифровой подписи.
19. Протоколы сертификации ключей.
20. Протоколы предварительного распределения ключей.
21. Протоколы выработки сеансовых ключей.
22. Открытое распределение ключей Диффи-Хеллмана и его модификации.

Повышенный уровень

Тема 11. Сложность криптографических алгоритмов.
1. Способы определения сложности алгоритмов.
2. Сложность известных алгоритмов, используемых в криптографии и криптоанализе.
Тема 13. Криптосистемы на основе метода эллиптических кривых.
3. Криптосистемы на основе метода эллиптических кривых.
Тема 14. Аутентификация данных. Электронная цифровая подпись.
4. Атаки и угрозы схемам ЭЦП.
5. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.

Тема 16. Понятие о структуре и способах построения криптографических протоколов.
6. Атаки на криптографические протоколы. Виды атак, способ подмены пользователя сети, способ замены долговременного ключа.
7. Способы отражения атак на криптографические протоколы.

1. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если он в ходе собеседования правильно ответил на вопрос по теме собеседования, сопровождая наглядными примерами.
Оценка «хорошо» выставляется студенту, если он в ходе собеседования ответил на вопрос по теме собеседования, при этом есть неуверенность с практическими примерами.
Оценка «удовлетворительно» выставляется студенту, если он ходе собеседования ответил неуверенно на вопросы по теме собеседования, не смог привести практические примеры.
Оценка «неудовлетворительно» выставляется студенту, если он не ответил на вопрос по теме собеседования.

2. Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура проведения данного оценочного мероприятия включает в себя устные ответы студентов на вопросы собеседования.

Предлагаемые студенту вопросы позволяют проверить компетенции ОПК-2, ОПК-4, ПК-1.

Каждому студенту предлагается ответить на два вопроса базового уровня и один вопрос повышенного уровня.

При подготовке к ответу студенту предоставляется право пользования лекциями, и методическими материалами к самостоятельной работе.

При оценивании ответов студента учитываются:

- точность и последовательность формулировок;
- умение приводить конкретные примеры по теме вопроса.

Составитель _____ Н.И. Битюцкая
(подпись)

«____»_____20 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске
Кафедра информационной безопасности, систем и технологий

УТВЕРЖДАЮ:
Зав. кафедрой ИБСиТ
_____ В.Ф. Антонов
«__» _____ 2020 г.

Вопросы к экзамену

по дисциплине «Криптографические методы защиты информации»

6 семестр

Базовый уровень

Вопросы (задача, задание) для проверки уровня обученности.

Знать

1. Основные понятия в области криптографии.
2. Классификация классических шифров: шифры замены и перестановки, поточные и блочные шифры, моноалфавитные и многоалфавитные шифры.
3. Классические шифры с симметричным ключом. Шифры замены: аддитивные, мультипликативные, аффинные, автоключевой, Виженера, Плейфера, Хилла, роторный, одноразового блокнота.
4. Классические шифры перестановки: бесключевой шифр, ключевые шифры и шифры с двойной перестановкой.
5. Современные блочные шифры с симметричным ключом. Основные компоненты современного блочного шифра. Шифры Фейстеля и не-Фейстеля.
6. Современные поточные шифры с симметричным ключом. Синхронные и несинхронные шифры потока. Преимущества и проблемы современных шифров потока.
7. Современный стандарт шифрования (DES). Структура шифра DES. Раунды шифрования. Функция DES. Генерация ключей раундов.
8. Усовершенствованный стандарт шифрования (AES). Алгоритм расширения ключей. Анализ расширения ключа. Алгоритмы шифрования и дешифрования в AES.
9. Российский стандарт ГОСТ 2847-89, особенности, принципы построения, методы шифрования.
10. Алгоритмы шифрования с открытыми ключами. Концепция криптографии с открытым ключом. Криптосистема RSA. Стойкость RSA.
11. Алгоритмы генерации простых чисел. Проверка чисел на простоту. Способы проверки на простое число. Решето Эратосфена. Phi-функция Эйлера. Простые числа Мерсенны. Простые числа Ферма. Детерминированные и вероятностные алгоритмы проверки чисел на простоту.
12. Сложность криптографических алгоритмов. Понятие сложности алгоритма. Линейная, полиномиальная и неполиномиальная сложность. Класс NP – полных задач.
13. Криптосистемы с открытым ключом. Криптосистема Рабина. Криптосистема Эль-Гамаля. Алгоритмы шифрования, дешифрования и генерации ключей в криптосистемах Рабина и Эль-Гамаля. Безопасность данных криптосистем.

14. Аутентификация данных. Электронная цифровая подпись. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП.
15. Алгоритмы ЭЦП: RSA, Эль-Гамаля, ФиатаШамира, Онга-Шнорра-Шамира, Шнорра. Неотрицаемая подпись Шаума-ванАнтверпена.
16. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.9.
17. Генерация и проверка цифровой подписи на основе криптосистемы Эль-Гамаля. Алгоритм формирования схемы Эль-Гамаля. Алгоритм формирования цифровой подписи. Проверка подписи.
18. Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. Парольные схемы и протоколы "рукопожатия".
19. Взаимосвязь между протоколами аутентификации и цифровой подписи. Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификации.

Уметь
1. Шифровать тексты с помощью классических шифров.
2. Шифровать двоичные последовательности с помощью современных шифров.
3. Проверять требования к криптосистемам.
4. Использовать перестановки, подстановки и их комбинации.
5. Реализовывать криптографические методы.

Владеть
1. Методами управления ключами.
2. Методами генерации, накопления и распределения ключей.
3. Основами знаний по порядку разработки схемы ЭЦП Рабина.
4. Основами знаний по порядку разработки схемы ЭЦП Диффи - Хэллмана.
5. Основами знаний по порядку разработки схемы ЭЦП Эль-Гамаля.

Повышенный уровень

Вопросы (задача, задание) для проверки уровня обученности.

Знать
1. Виды атак криптоанализа. Способы противодействия им.
2. Криптоанализ шифров замены.
3. Криптоанализ шифров перестановки.
4. Атаки на современные блочные шифры.
5. Криптоанализ современных шифров потока.
6. Двукратный и трехкратный DES. Криптоанализ шифра DES.
7. Анализ AES.
8. Виды атак на RSA.
9. Способы определения сложности алгоритмов.
10. Сложность известных алгоритмов, используемых в криптографии и криптоанализе.
11. Криптосистемы на основе метода эллиптических кривых.
12. Безопасность криптосистемы с эллиптической кривой.
13. Атаки на криптографические протоколы. Виды атак, способ подмены пользователя сети, способ замены долговременного ключа.
14. Способы отражения атак на криптографические протоколы.

Уметь
1. Отражать атаки на криптографические протоколы.
2. Выбирать правильно параметры для шифрования наиболее известными шифрами.

3. Оценивать криптостойкость алгоритма шифрования.

Владеть 1. Способами построения криптографических протоколов.
2. Способами отражения атак на криптографические протоколы.

1. **Критерии оценивания компетенций**

Оценка «отлично» выставляется студенту, если теоретическое содержание курса освоено полностью, без пробелов; исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует в ответе дополнительный материал, все предусмотренные программой задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному; анализирует полученные результаты; проявляет самостоятельность при выполнении заданий.

Оценка «хорошо» выставляется студенту, если теоретическое содержание курса освоено полностью, необходимые практические компетенции в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.

Оценка «удовлетворительно» выставляется студенту, если теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, большинство предусмотренных программой заданий выполнено, но в них имеются ошибки, при ответе на поставленный вопрос студент допускает неточности, недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении программного материала.

Оценка «неудовлетворительно» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, необходимые практические компетенции не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, качество их выполнения оценено числом баллов, близким к минимальному.

2. Описание шкалы оценивания

Промежуточная аттестация в форме **экзамена** предусматривает проведение обязательной экзаменационной процедуры и оценивается 45 баллами из 100. Минимальное количество баллов, необходимое для допуска к экзамену, составляет 33 балла. Положительный ответ студента на экзамене оценивается рейтинговыми баллами в диапазоне от **20** до **45** (**20**$\leq S_{экз} \leq$**45**), оценка **меньше 20** баллов считается неудовлетворительной.

Шкала соответствия рейтингового балла экзамена 5-балльной системе

Рейтинговый балл по дисциплине	**Оценка по 5-балльной системе**
37 – 45	Отлично
28 – 36	Хорошо
20 – 27	Удовлетворительно

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура проведения **экзамена** осуществляется в соответствии с Положением о

проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования в СКФУ.

В экзаменационный билет включаются два теоретических вопроса базового и один повышенного уровня.

Для подготовки по билету отводится от 40 до 60 минут.

При подготовке к ответу студенту предоставляется право пользования собственными лекциями, а также любой справочной литературой в течение 3-5 минут.

Составитель _____ Н.И. Битюцкая

«____»_____20 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зав. кафедрой ИБСиТ

_____ В.Ф. Антонов

«____» _____ 202_ г.

Темы индивидуальные заданий для лабораторных работ по дисциплине «Криптографические методы защиты информации»

5 семестр

Базовый уровень

1. Вычисление наибольшего общего делителя для двух чисел при помощи алгоритма Евклида.
2. Расширенный алгоритм Евклида.
3. Нахождение мультипликативной инверсии числа по заданному модулю с использованием расширенного алгоритма Евклида.
4. Решение линейного диофантового уравнения с использованием расширенного алгоритма Евклида.
5. Решение уравнения сравнения с использованием расширенного алгоритма Евклида.
6. Программная реализация классических шифров замены с симметричным ключом.
7. Программная реализация классических шифров перестановки с симметричным ключом.
8. Программная реализация основных компонентов современных блочных шифров с симметричным ключом.

Повышенный уровень

1. Программная реализация шифра Хилла.
2. Программная реализация роторного шифра.
3. Программная реализация ключевого шифра с двойной перестановкой.
4. Программная реализация шифра DES.

6 семестр

Базовый уровень

1. Программная реализация генератора простых чисел.
2. Программная реализация шифра RSA.
3. Программная реализация ЭЦП.
4. Программная реализация криптографических протоколов.

Повышенный уровень

1. Протокол Диффи-Хеллмана для эллиптических кривых.
2. Электронная цифровая подпись на эллиптических кривых.

1. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если отчет по работе выполнен в соответствии с требованиями, предъявляемыми методическими рекомендациями по выполнению лабораторных работ, а также раскрыты полностью все вопросы по заданию.

Оценка «хорошо» выставляется студенту, если отчет по работе выполнен в соответствии с требованиями, предъявляемыми методическими рекомендациями по выполнению лабораторных работ, а также частично раскрыты вопросы по заданию.

Оценка «удовлетворительно» выставляется студенту, если отчет по работе выполнен в соответствии с требованиями, предъявляемыми методическими рекомендациями по выполнению лабораторных работ, а также раскрыт не полностью перечень необходимых вопросов по заданию.

Оценка «неудовлетворительно» выставляется студенту, если отчет по работе выполнен не в соответствии с требованиями, предъявляемыми методическими рекомендациями по выполнению лабораторных работ, а также не раскрыты вопросы по заданию.

2. Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура проведения данного оценочного мероприятия включает в себя: выполнение индивидуального задания и оформление отчета по лабораторным работам. Предлагаемые студенту задания позволяют проверить компетенции ОПК-2, ОПК-4, ПК-1.

Для подготовки к данному оценочному мероприятию необходимо к концу текущей лабораторной работы предоставить отчет по выполнению лабораторной работы.

При подготовке к ответу студенту предоставляется право пользования справочными материалами.

При проверке задания, оцениваются:

- последовательность и рациональность выполнения;
- знания технологий, использованных при выполнении задания,
- оформление отчета по лабораторной работе.

Составитель _____ Н.И. Битюцкая

«____»_____20 г.

Оценочный лист

№ п/п	Ф.И.О. студента	Параметры состояния образованности									Итоговый балл
		Предметно-информационная составляющая образованности				Деятельностно-коммуникативная составляющая образованности			Ценностно-ориентационная составляющая образованности		
		Контрольно-методический срез	Общеучебные умения и навыки			Уровень развития устной речи	Умение работать с информацией	Грамотность	Умение использовать получен-ные знания в повседневной жизни	Уровень адекватности самооценки	
			Умение анализировать	Умение доказывать	Умение делать выводы						
1.	Абрамов Станислав										
2.	Багно Елизавета										
3.	Бойко Денис										
4.	Вардазарян Гор										
5.	Калабеков Исмаил										
6.	Каспарян Геворг										
7.	Клюев Дмитрий										
8.	Кононенко Александр										
9.	Конопляник Антон										
10.	Рокшин Владислав										
11.	Русанов Владислав										
12.	Тарабанова Мария										
13.	Тарочкин Артем										
14.	Трубаев Артем										
15.	Хадзегова Зарина										
16.	ЯновТамирлан										