ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ

**«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ГУМАНИТАРНО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»**

КАЛМЫЦКИЙ ФИЛИАЛ

УТВЕРЖДАЮ
Директор филиала
_____Э.Л. Пашнанов
«23» 04 2020 г.

ПРОГРАММА ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ «КИБЕРБЕЗОПАСНОСТЬ»

Элиста 2020 г.

Разработчик:

Пипенко В.В., преподаватель первой квалификационной категории, Калмыцкий филиал ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет»

Рецензент:

Агеев С.С., заместитель начальника отдела обеспечения деятельности, противодействия коррупции кадров и защиты информации, Министерства финансов Республики Калмыкия

Рассмотрено на заседании предметно-цикловой комиссии естественнонаучных и математических дисциплин

протокол № 7 от «22» 04 2020 г.
Председатель ПЦК _____ /Катрикова Ц.Ю./

Программа обсуждена и одобрена научно-методическим советом Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет».
Протокол № 5 от 23.04 2020 г.

Дополнительная профессиональная программа повышения квалификации «Кибербезопасность» (далее – программа) определяет требования к содержанию и уровню подготовки слушателя, виды учебных занятий по реализации учебного процесса, руководство самостоятельной работой слушателей и формы контроля по данному курсу.

Программа подготовлена для индивидуальных предпринимателей и включает в себя:

1. Общая характеристика программы.

1.1. Цель реализации программы.

1.2. Задачи преподавателя программы.

1.3. Требования к уровню образования лиц, допускаемых к освоению программы.

2. Требования к результатам освоения программы.

Планируемые результаты освоения программы.

3. Содержание программы

3.1. Учебный план.

3.2. Учебно-тематический план.

4. Календарный учебный график.

5. Рабочая программа дисциплины.

6. Организационно-педагогические условия реализации программы.

6.1. Кадровое обеспечение программы.

6.2. Методические рекомендации преподавателю.

6.3. Методические указания слушателю.

7. Формы аттестации.

8. Оценочные материалы.

9. Методическое обеспечение программы.

10. Материально-техническое обеспечение программы.

1. Общая характеристика программы

1.1. Цель реализации программы

Дополнительная профессиональная программа дополнительного образования «Кибербезопасность» направлена на формирование общих представлений о безопасности в информационном обществе и на этой основе сформировать понимание технологий информационной безопасности и умения применять правила кибербезопасности во всех сферах деятельности.

Программа разработана в соответствии с:

– Федеральным законом РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

– Федеральным законом РФ «О конкуренции и ограничении монополистической деятельности на товарных рынках» от 06.05.98 №70-ФЗ.

– Федеральным законом РФ «О рекламе» от 13.03.2006 №38-ФЗ (с учетом дополнений и изменений).

– Приказом Минобрнауки России от 01.07.2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

– Письмом Минэкономразвития России N 5594-ЕЕ/Д28и, Минобрнауки России № АК-553/06 от 12.03.2015 «О направлении методических рекомендаций»;

– Письмом Минобрнауки России от 22.04.2015 № ВК-1032/06 «О направлении методических рекомендаций» (вместе с «Методическими рекомендациями-разъяснениями по разработке дополнительных профессиональных программ на основе профессиональных стандартов»);

1.2. Задачи программы

- формирование общих представления о безопасности в информационном обществе;
- описать общие принципы технологий, применяемых в информационной безопасности;
- привить умения применять правила кибербезопасности во всех сферах деятельности;
- освоение знаний, составляющих начала представлений об информационной картине мира и информационных процессах;
- овладение умением использовать компьютерную технику как практический инструмент для
- работы с информацией в повседневной жизни;
- развитие навыков ориентирования в информационных потоках.

1.3. Требования к уровню образования лиц, допускаемых к освоению программы

К освоению программы повышения квалификации допускаются:

1) лица, имеющие среднее профессиональное и (или) высшее образование;

2) лица, получающие среднее профессиональное и (или) высшее образование.

2. Требования к результатам освоения программы. Планируемые результаты освоения программы

В результате освоения программы слушатель должен обладать: общими компетенциями, включающие в себя способность:

ОК – 2. Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество;

ОК – 3. Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях;

ОК – 4. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и

решения профессиональных задач, профессионального и личностного развития;

ОК – 5. Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности;

ОК – 7. Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий;

профессиональными компетенциями, соответствующие видам деятельности:

ПК – 1. Способен разрабатывать модели средств, систем и процессов в инфокоммуникациях, проверять их адекватность на практике и использовать пакеты прикладных программ анализа и синтеза инфокоммуникационных систем, сетей и устройств.

ПК – 13. Способен к выполнению работ по обеспечению функционирования телекоммуникационного оборудования корпоративных сетей с учетом требований информационной безопасности;

В результате освоения программы обучающийся должен демонстрировать следующие результаты обучения:

знать:

- объекты компьютерных технологий, используемые в обеспечении кибербезопасности;
- понятийный аппарат информационных технологий и особенности терминологии кибербезопасности;
- базовые составляющие в области развития систем информационной безопасности;

- объекты компьютерно-технической экспертизы;

уметь:

- ставить цели, формулировать задачи, связанные с обеспечением кибербезопасности;
- анализировать тенденции развития систем обеспечения кибербезопасности;
- применять знания о кибербезопасности в решении поставленных задач.

владеть:

- знаниями о современных технологиях, применяемых в области кибербезопасности;
- методами проведения анализа в области обеспечения кибербезопасности.

3. Содержание программы

3.1. Учебный план программы повышения квалификации «Кибербезопасность»

Категория слушателей: индивидуальные предприниматели, желающие освоить программу, имеющие среднее профессиональное или высшее образование, а также лица, получающие среднее профессиональное или высшее образование.

Срок обучения - 72 ч.

Форма обучения - очно-заочная

Режим занятий - 6 часов в день.

№ п/п	Наименование разделов (дисциплины, модули)	Всего, ч.	В том числе		Формы контроля
			лекции	практические занятия	
1	2	3	4	5	6
1.	Раздел 1. Компьютерные сети, информационно-аналитические системы и системы моделирования в технике	8	4	4	Текущий контроль (устный опрос)
2.	Раздел 2. Киберпространство и основы кбербезопасности, векторы риска	8	6	2	Текущий контроль (устный опрос)
3.	Раздел 3. Методы обеспечения безопасности ПК и интернета, вирусы и антивирусы	8	2	6	Текущий контроль (устный опрос)
4.	Раздел 4. Мошеннические действия в интернете, киберпреступления против личности, общества и государства, хакерские атаки и кибертерроризм	2	2	-	Текущий контроль (устный опрос)

5.	Раздел 5. Организация и проведение работ по технической защите информации в компьютерных сетях и системах	20	8	12	Текущий контроль (устный опрос)
6.	Раздел 6. Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации	20	8	12	Текущий контроль (устный опрос)
		6			демонстрационный экзамен
	ИТОГО	72	30	36	

3.2. Учебно-тематический план программы повышения квалификации «Кибербезопасность»

№ п/п	Наименование разделов (дисциплины, модули)	Всего, ч.	В том числе		Формы контроля
			лекции	практические занятия	
1	2	3	4	5	6
1	**Раздел 1. Компьютерные сети, информационно-аналитические системы и системы моделирования в технике**				
1.1.	Информационная безопасность. Функциональная безопасность. Уязвимости, угрозы и риски. Вредоносное программное обеспечение. Векторы и поверхности атаки. Последствия кибератак. Нетехнические способы компрометации систем безопасности. Социальная инженерия. Информационная безопасность. Функциональная безопасность. Уязвимости, угрозы и риски. Вредоносное программное обеспечение. Векторы и поверхности атаки. Последствия кибератак.	8	4	4	Текущий контроль (устный опрос)
2.	**Раздел 2. Киберпространство и основы кбербезопасности, векторы риска**				
2.1.	Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации. Проверка подлинности (аутентификация) в Интернете.	8	6	2	Текущий контроль (устный опрос)

	Меры безопасности для пользователя WiFi. Настройка безопасности. Настройка компьютера для безопасной работы. Ошибки пользователя. Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях				
3	**Раздел 3. Методы обеспечения безопасности ПК и интернета, вирусы и антивирусы**				
3.1.	Технологии защиты. Стратегии снижения рисков. Аудит безопасности. Мониторинг инцидентов кибербезопасности. Реагирование на инциденты кибербезопасности. Адаптивная архитектура безопасности.	8	2	6	Текущий контроль (устный опрос)
4	**Раздел 4. Мошеннические действия в интернете, киберпреступления против личности, общества и государства, хакерские атаки и кибертерроризм**				
4.1.	Кибератаки и техногенные катастрофы. Защита IT-инфраструктур критически важных объектов. Понятие и виды хакерских атак. Способы защиты от хакерских атак. Кибертерроризм: понятие, приемы, способы предотвращения.	2	2	-	Текущий контроль (устный опрос)
5	**Раздел 5. Организация и проведение работ по технической защите информации в компьютерных сетях и системах**				
5.1.	Организационно-технические мероприятия по защите информации. Вопросы проектирования, внедрения и эксплуатации АС и их систем зашиты информации.	20	8	12	Текущий контроль (устный опрос)
6	**Раздел 6. Проведение аттестации объектов вычислительной техники на**				

	соответствие требованиям по защите информации				
6.1.	Деятельность по аттестации объектов информатизации по требованиям безопасности информации. Добровольная и обязательная аттестация. Органы входящие в структуру системы аттестации. Документы и данные необходимые для проведения аттестации объектов вычислительной техники.	20	8	12	Текущий контроль (устный опрос)
	Итоговая аттестация.	6	-	-	**демонстрационный экзамен**
	Итого	72	30	36	

4. Календарный учебный график

Объем программы- 72 часа.

Продолжительность обучения – 2 недели, 12 рабочих дней.

Период обучения/учебные дни					
1	**2**	**3**	**4**	**5**	**6**
Р 1	Р 1,2	Р 2,3	Р 3	Р 4,5	Р 5
7	**8**	**9**	**10**	**11**	**12**
Р 5	Р 5,6	Р 6	Р 6	Р 6	ИА

*Примечание: Р – раздел с порядковым номером в соответствии с учебным планом, ИА – итоговая аттестация.

5. Рабочая программа дисциплины

Раздел 1. Компьютерные сети, информационно-аналитические системы и системы моделирования в технике

Информационная безопасность. Функциональная безопасность. Уязвимости, угрозы и риски. Вредоносное программное обеспечение. Векторы и поверхности атаки. Последствия кибератак. Нетехнические способы компрометации систем безопасности. Социальная инженерия. Информационная безопасность. Последствия кибератак.

Практические занятия

Функциональная безопасность. Уязвимости, угрозы и риски. Вредоносное программное обеспечение. Векторы и поверхности атаки.

Раздел 2. Киберпространство и основы кибербезопасности, векторы риска

Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации. Проверка подлинности (аутентификация) в Интернете. Меры безопасности для пользователя WiFi. Настройка безопасности. Ошибки пользователя. Меры личной безопасности при сетевом общении.

Практические занятия

Настройка компьютера для безопасной работы. Настройки приватности в социальных сетях

Раздел 3. Методы обеспечения безопасности ПК и интернета, вирусы и антивирусы

Технологии защиты. Стратегии снижения рисков. Аудит безопасности. Мониторинг инцидентов кибербезопасности. Реагирование на инциденты кибербезопасности. Адаптивная архитектура безопасности.

Практические занятия

Аудит безопасности. Мониторинг инцидентов кибербезопасности. Реагирование на инциденты кибербезопасности.

Раздел 4. Мошеннические действия в интернете, киберпреступления против личности, общества и государства, хакерские атаки и кибертерроризм

Кибератаки и техногенные катастрофы. Защита IT-инфраструктур критически важных объектов. Понятие и виды хакерских атак. Способы защиты от хакерских атак. Кибертерроризм: понятие, приемы, способы предотвращения.

Раздел 5. Организация и проведение работ по технической защите информации в компьютерных сетях и системах

Организационно-технические мероприятия по защите информации. Вопросы проектирования, внедрения и эксплуатации АС и их систем зашиты информации.

Практические занятия

Проектирование, внедрение и эксплуатации АС и их систем зашиты информации

Раздел 6. Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации

Деятельность по аттестации объектов информатизации по требованиям безопасности информации. Добровольная и обязательная аттестация. Органы входящие в структуру системы аттестации. Документы и данные необходимые для проведения аттестации объектов вычислительной техники.

6. Организационно-педагогические условия реализации программы

6.1. Кадровое обеспечение программы

В реализации дополнительной профессиональной программы повышения квалификации «Интернет маркетинг для бизнеса» участвуют преподаватели, имеющие высшее образование, соответствующее профилю преподаваемой дисциплины и богатый опыт деятельности в области построения маркетинговых стратегий с использованием Интернет сервисов, в

том числе:

Ф.И.О.	Должность	Ученая степень/ученое звание
Пипенко В.В.	Преподаватель первой категории, эксперт демонстрационного экзамена по компетенции «Кибербезопасность»	-
		-
		-

6.2. Методические рекомендации преподавателю

Программа повышения квалификации «Кибербезопасность» разработана для проведения занятий в Калмыцком филиале МГГЭУ со слушателями, из числа граждан, зарегистрированных в качестве индивидуальных предпринимателей, желающих освоить программу.

Основными видами аудиторной работы слушателей являются: лекции и практические занятия.

В ходе лекции преподаватель излагает и разъясняет основные положения темы, связанные с ней теоретические и практические проблемы, дает рекомендации к практической деятельности.

При проведении практических занятий преподаватель должен четко формулировать цель занятия и основные проблемные вопросы. После заслушивания ответов слушателей необходимо подчеркнуть положительные аспекты их работы, обратить внимание на имеющиеся неточности (ошибки), дать рекомендации по дальнейшей подготовке.

В целях контроля уровня подготовленности слушателей, для закрепления теоретических знаний и привития им навыков работы по предложенной тематике преподаватель в ходе лекции и практических занятий может проводить устные опросы, давать письменные практические задания, с помощью которых преподаватель проверяет умение применять полученные знания для решения конкретных задач.

Преподаватель должен осуществлять индивидуальный контроль работы слушателей; давать соответствующие рекомендации; в случае необходимости помочь слушателю составить индивидуальный план работы по изучению данной программы.

6.3. Методические указания слушателю

Основными видами аудиторной работы слушателей при изучении дополнительной профессиональной программы дополнительного образования «Кибербезопасность» являются лекции и практические занятия.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. Слушатель не имеет права пропускать без уважительных причин аудиторные занятия, в противном случае он может быть не допущен к итоговой аттестации.

При изучении тем учебной программы применяются практические занятия, цель которых заключается в достижении более глубокого, полного усвоения учебного материала, а также развитие навыков самообразования. Кроме того, практические занятия служат формой контроля преподавателем уровня подготовленности слушателя, закрепления изученного материала, выработки навыков и умений применять полученные знания для решения имеющихся и вновь возникающих профессиональных задач.

При реализации вышеуказанных форм изучения материала курсов повышения квалификации предусматриваются следующие виды самостоятельной работы слушателей:

- работа с учебно-методическими пособиями (конспектом лекций);
- работа с рекомендованной литературой;
-работа в сети интернет;
-подготовка к итоговой аттестации.

7. Формы аттестации

Текущий контроль осуществляется преподавателем, ведущим лекционные и практические занятия, после изучения каждого модуля в виде устного опроса. Результаты текущего контроля являются допуском слушателя к итоговой аттестации или отчислению за невыполнение учебного плана.

Завершающей стадией обучения является итоговая аттестация в форме демонстрационного экзамена в виде выполнения практической работы в целях контроля уровня освоения программы. К итоговой аттестации допускается слушатель, не имеющий задолженности и в полном объеме выполнивший учебный план по программе. Итоговая аттестация может проводится как на бумажных носителях, так с использованием специальных программ. Итоговая аттестация слушателей осуществляется итоговой аттестационной комиссией, созданной Калмыцким филиалом МГГЭУ. Результаты итоговой аттестации определяются итоговой аттестационной комиссией по результатам выполненных тестовых заданий на последнем занятии.

Слушатели, успешно освоившие программу и прошедшие итоговую аттестацию, получают удостоверение о повышении квалификации.

8. Оценочные материалы

С целью проверки знаний по программе повышения квалификации «Кибербезопасность» используются следующие методы: для текущего

контроля - устный опрос, для итоговой аттестации – демонстрационный экзамен.

Оценочные материалы для текущего контроля в форме устного опроса:

1. Национальные стандарты России в области киберпезопасности;
2. проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации;
3. характеристика современного вредоносного программного обеспечения и виды кибератак;
4. новые технологии и новые угрозы информационной безопасности;
5. особенности современных информационных систем как объекта защиты информации;
6. основные международные стандарты и наборы рекомендаций в области проектного и процессного управления;
7. основные угрозы, риски и уязвимости в сфере кибербезопасности и критической информационной инфраструктуры;
8. основные понятия в сфере функциональной безопасности;
9. положения основных нормативных актов, регулирующих сферу безопасности критической информационной инфраструктуры Российской Федерации;
10. архитектура основных подсистем обеспечения ИБ объектов КИИ;
11. основные определения СМИБ и особенности построения СМИБ для объектов КИИ на промышленных объектах;
12. положения нормативных актов, устанавливающих ответственность за нарушение требований законодательства РФ в сфере обеспечения безопасности КИИ и КВО ТЭК.
13. основные средства обеспечения кибербезопасности (архитектура, принципы построения);
14. принципы проектирования систем безопасности значимых объектов КИИ;
15. состав и способы организации деятельности сил обеспечения кибербезопасности объектов КИИ;
16. основные риски и проблемы усовершенствования системы кибербезопасности;
17. состав и классификация систем для «Умного города», критерии оценки безопасности, основных угроз, рисков и проблем, структуры и особенностей построения модели угроз.

Текущий контроль в форме устного опроса оценивается по двухбалльной системе: «зачет», «незачет».

Критерии оценивания устного опроса:

Оценка «зачет» ставится, если:

- в ответах на вопросы при раскрытии содержания вопросов раскрываются и анализируются основные противоречия и проблемы;

- при раскрытии особенностей развития тех или иных профессиональных идей, а также описания профессиональной деятельности используются материалы современных пособий и первоисточников, допускаются фактические ошибки;

- представление профессиональной деятельности в полном объеме или частично рассматривается в контексте собственного профессионального опыта, практики его организации;

- при ответе используется терминология и дается ее определение, соответствующая конкретному периоду развития теории и практики профессиональной деятельности;

- ответы на вопросы имеют логически выстроенный характер, используются такие мыслительные операции, как сравнение, анализ и обобщение;

- имеется личная точка зрения слушателя, основанная на фактическом и проблемном материале, приобретенной на лекционных и практических занятиях и в результате самостоятельной работы.

Оценка «незачет» ставится, если:

- при ответе обнаруживается отсутствие владением материалом в объеме изучаемой образовательной программы;

- при раскрытии особенностей развития тех или иных профессиональных идей не используются материалы современных источников;

- представление профессиональной деятельности не рассматривается в контексте собственного профессионального опыта, практики его организации;

- при ответе на вопросы не дается трактовка основных понятий;

- ответы на вопросы не имеют логически выстроенного характера, не используются такие мыслительные операции, как сравнение, анализ и обобщение.

Оценочные материалы для итоговой аттестации:

Модуль 1:

Защита корпоративной ИТ-инфраструктуры Компания «ООО DE F8» делегировала Вам полномочия на развертывании сетевой инфраструктуры, повышения безопасности внутри нее, а также разграничения прав в демилитаризированной зоне (DMZ) и на сетевом оборудовании. В том числе Вам предстоит настроить сетевое оборудование (Коммутатор). IT отдел предоставил Вам топологию сети компании с ее необходимыми параметрами для дальнейшего построения защищенной сети. В Вашем распоряжении имеются все необходимые виртуальные машины и образы для выполнения задания. По завершении работы необходимо подготовить отчет REPORT_DAY_1, в отчете указать устанавливаемые логины и пароли.

Время выполнения модуля: 6 часов

Критерии оценивания итоговой аттестации:

Общее максимально возможное количество баллов задания по всем

критериям оценки составляет 66.

№ п/п	Критерий	Модуль в котором используются критерии	Проверяемые разделы WSSS	Баллы		
				Судейская (если это применимо)	Объективная	Общая
1	Защита корпоративной ИТ инфраструктуры	1	1 2 3	4	62	66
Итого =				**4**	**62**	**66**

9. Методическое обеспечение программы

9.1. Нормативные правовые акты

1. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

9.2. Основная литература

2. Петренко С. А., Смирнов М. Б. Безопасность АСУТП и критической информационной инфраструктуры // СПб.: ООО «ИД «Афина». – 2018. ISBN 978-5-9909868-1-7. Учебно-методическое пособие
3. Федорова Г.Н. Разработка, администрирование и защита баз данных: учебник для студ. учреждений сред. проф. образования – 4-е изд., стер. – М.: Издательский центр «Академия», 2020 - 288 с.
4. Семакин И.Г., Шестаков А.П. Основы алгоритмизации и программирования: учебник для студ. учреждений сред. проф. образования - 4-е изд., стер. — М.: Издательский центр "Академия", 2017
5. Немцова Т. И., Назарова Ю. В. Компьютерная графика и web-дизайн. Практикум: учебное пособие – М: ИД «ФОРУМ»: ИНФРА-М, 2010. — 288 с.: ил. — (Профессиональное образование).

9.3 Дополнительная литература

6. Дроздов С. EurotEch, «Интернет вещей» и «облако устройств» / С. Дроздов, С. Золотарев // Control Engineering. – 2012. – № 8. – С.19.
7. Маркеева А.В. Интернет вещей (iot): возможности и угрозы для современных организаций / А.В. Маркеева // Общество: социология, психология, педагогика. – 2016. – № 2. – С. 42–46.
8. Лаврова Д.С. Обнаружение инцидентов безопасности в Интернете Вещей / А.И. Печенкин, Д.С. Лаврова // Проблемы информационной безопасности. Компьютерные системы. – СПб.: Изд-во Политехн. Ун-та. – 2015. – №2. – С. 69-79.

9.4 Интернет - ресурсы:

1. Интернет-ресурс Центрального банка России URL: www.cbr.ru
2. Сайт информационного агентства АК&M. URL: www.akm.ru
3. Интернет-ресурс «Инновации - инвестиции – индустрия». URL: http://www.rvca.ru

4. Универсальный портал для экономистов. URL: http://www.cfin.ru
5. Технологии управления проектами. URL: http://www.project.km.ru/

10. Материально-технические условия реализации программы

Учебно-методическое обеспечение:

- набор электронных презентаций для использования в аудиторных занятиях;
- тестовые материалы (для проведения электронного тестирования);
- дидактические материалы в электронном виде;
- набор оценочных средств для контроля усвоения материала по темам программы.

Материально-техническое обеспечение

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
Аудитория	Лекции	Автоматизированное рабочее место: не менее Core i5, 8GB ОЗУ, 1TB HD, Монитор 24", ИБП на 650Вт, мультимедийный проектор, экран, интерактивная доска. Набор электронных презентаций для использования в аудиторных занятиях. МФУ. Автоматизированное рабочее место преподавателя. Автоматизированные рабочие места обучающихся.
Мастерская по компетенции «Кибербезопасность»	Практические занятия	Автоматизированное рабочее место преподавателя: не менее Core i5, 8GB ОЗУ, 1TB HD, Монитор 22", ИБП на 650Вт Автоматизированные рабочие места обучающихся: не менее Core i5, 8GB ОЗУ, 1TB HD, Монитор 22", ИБП на 650Вт.
Мастерская по компетенции «Кибербезопасность»	Итоговая аттестация	Автоматизированное рабочее место: не менее Core i5, 8GB ОЗУ, 1TB HD, Монитор 22", ИБП на 650Вт, мультимедийный проектор, экран, интерактивная доска. Автоматизированное рабочее место

		преподавателя: не менее Core i5, 8GB ОЗУ, 1TB HD, Монитор 22", ИБП на 650Вт Автоматизированные рабочие места обучающихся: не менее Core i5, 8GB ОЗУ, 1TB HD, Монитор 22", ИБП на
Программное обеспечение		Notepad ++ Sublime Text 3 Library / Framework Web Browser - Internet Explorer 10, Firefox, Chrome Discord или аналог Openvpn или аналог Google Диск или аналог TeamViewer или аналог