

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Кафедра вычислительной техники и защиты информации

**АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ
УЧЕБНОЙ ДИСЦИПЛИНЫ
«ЭКСПЕРТНЫЕ СИСТЕМЫ КОМПЛЕКСНОЙ
ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ»**

Уровень подготовки: высшее образование – магистратура

Направление подготовки
10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
(код и наименование направления подготовки)

Направленность подготовки
Информационная безопасность
(наименование программы подготовки)

Квалификация (степень) выпускника
Магистр
Форма обучения
очная

Разработана в соответствии
с ФГОС ВПО, Приказ МОиН РФ от 28.10.2009, № 497
Актуализирована в соответствии
с ФГОС ВО, Приказ МОиН РФ от 01.12.2016, № 1513

Уфа 2016

Исполнитель
профессор кафедры ВТ и ЗИ  В. И. Васильев

Заведующий кафедрой
вычислительной техники и защиты информации  В. И. Васильев

1. Место дисциплины в структуре образовательной программы

Дисциплина «Экспертные системы комплексной оценки безопасности информационно-телекоммуникационных систем» является обязательной дисциплиной вариативной части ОПОП по направлению подготовки «Информационная безопасность», направленность «Информационная безопасность».

Рабочая программа составлена в соответствии с требованиями:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки 090900 Информационная безопасность (квалификация "магистр"), утвержденного приказом Министерства образования и науки Российской Федерации от 28 октября 2009 г. № 497;
- Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки 10.04.01 Информационная безопасность (квалификация "магистр"), утвержденного приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г. № 1513.

Является неотъемлемой частью основной образовательной профессиональной программы (ОПОП).

Целью освоения дисциплины является получение обучающимися систематизированных теоретических знаний об основных методах и способах оценки уровня защищенности сложных информационно-телекоммуникационных систем с использованием экспертных систем, освоение ими типовых программных средств автоматизации аудита информационной безопасности вычислительных систем и сетей, привитие базовых навыков оценки безопасности информационно-телекоммуникационных систем с использованием методов и технологий искусственного интеллекта.

Задачи:

- изучить основные методы и способы комплексной оценки безопасности информационно-телекоммуникационных систем с использованием технологий экспертных систем;
- формирование умения ставить и решать задачи аудита информационной безопасности информационно-телекоммуникационных систем с использованием типовых программных продуктов и систем;
- формирование навыков оценки безопасности информационно-телекоммуникационных систем с использованием методов и технологий искусственного интеллекта.

Входные компетенции:

На пороговом уровне ряд компетенций был сформирован за счет обучения на предыдущих уровнях высшего образования (бакалавриат, специалист)

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции*	Название дисциплины (модуля), практики, научных исследований, сформировавших данную компетенцию
1	способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения.	ОК-2	пороговый уровень первого этапа освоения компетенции	Научный семинар

*- **пороговый уровень** дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;

-базовый уровень позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;

-повышенный уровень предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.

Исходящие компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции*	Название дисциплины (модуля), практики, научных исследований, сформировавших данную компетенцию
1	способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	ПК-4	продвинутый уровень, конечный этап	ГИА

2. Перечень результатов обучения

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций.

Планируемые результаты обучения по дисциплине

№	Формируемые компетенции	Код	Знать	Уметь	Владеть
1	способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	ПК-4	основные методы и способы комплексной оценки безопасности информационно-телекоммуникационных систем ЧС использованием технологий экспертных систем	ставить и решать задачи аудита информационной безопасности информационно-телекоммуникационных систем с использованием типовых программных продуктов и систем	навыками оценки безопасности информационно-телекоммуникационных систем с использованием методов и технологий искусственного интеллекта

3. Содержание и структура дисциплины (модуля)

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 часов).

Трудоемкость дисциплины по видам работ

Вид работы	Трудоемкость, час.	
	1 семестр 180 часов /5 ЗЕ	2 семестр
Лекции (Л)	16	-
Практические занятия (ПЗ)	30	-
Лабораторные работы (ЛР)	8	-
КСР	5	-
Самостоятельная работа (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и	112	-

практическим занятиям, коллоквиумам, рубежному контролю и т.д.)(СРС)		
Подготовка и сдача экзамена	-	-
Подготовка и сдача зачета	9	-
Вид итогового контроля (зачет, экзамен)	зачет	-

Содержание разделов и формы текущего контроля

№	Наименование и содержание раздела	Количество часов						Литература, рекомендуемая студентам*	Виды интерактивных образовательных технологий**
		Аудиторная работа		СРС	Всего				
		Л	ПЗ						
1	Основные понятия в области информационно-телекоммуникационных систем и их защищенности от деструктивных воздействий	2	2	-	-	20	24	лекция классическая, лекция проблемная при проведении практических занятий: - проблемное обучение; - обучение на основе опыта	
1.1	Информационно-телекоммуникационная система (ИТКС), инфраструктура ИТКС, информационные ресурсы и информационные технологии в ИТКС	1	-	-	-	8	9	Р.6.1, № 1, гл. 1 Р.6.1, № 3, гл. 1,2,8 Р.6.2, № 3, гл. 1	
1.2	Требования к безопасности ИТКС. Конфиденциальность, целостность и доступность информации в ИТКС. Классификация информационных ресурсов в ИТКС по видам тайны (государственной, коммерческая тайна, конфиденциальная информация, персональные данные). Угрозы, уязвимости, информационные риски.	1	2	-	-	12	15	Р.6.1, № 1, гл. 1,2 Р.6.1, № 3, гл. 4-8 Р.6.2, № 8,9	
2	Нормативные документы в области информационной безопасности (ИБ) ИТКС	4	6	-	-	30	40		
2.1	Федеральные законы по защите информации. Руководящие документы Гостехкомиссии при Президенте РФ (ФСТЭК России)	2	2	-	-	15	19	Р.6.1, № 1, гл. 1 Р.6.2, № 8, 9	
2.2	Международная система стандартов в области ИБ. Национальные стандарты в области ИБ.	2	4	-	-	15	21	Р.6.2, № 2, гл. 2 Р.6.2, № 8,9	
3	Аудит ИБ ИТКС. Системы автоматизации проведения аудита ИБ	2	6	8	-	40	62		
3.1	Виды аудита ИБ. Системы поддержки принятия решений при проведении аудита ИБ (SRAMM, OSTATE, КОНДОР, ГРИФ, MIST). Требования к аудиту ИБ	2	6	8	-	24	41	Р.6.1, № 1, гл. 1,2 Р.6.1, № 3, гл. 3,18 Р.6.2, № 1, гл. 1-4 Р.6.2, № 3, гл. 3,4 Р.6.2, № 8,9	

3.2	Аудит ИС ПДн. Нормативная база проведения аудита ИС ПДн. Интеллектуальные системы поддержки принятия решений при аудите ИС ПДн	2	4	-	-	16	22	Р.6.1, № 1, гл. 1,2 Р.6.1, № 2, гл. 1,2 Р.6.2, № 1, гл. 1,2 Р.6.2, № 3, гл. 1-4 Р.6.2, № 4, гл. 10-12 Р.6.2, № 5, гл. 1-3
4	Экспертные системы комплексной оценки безопасности ИТКС	6	12	-	-	22	45	
4.1	Автоматизация процессов мониторинга и контроля ИБ ИТКС. Основные проблемы и пути решения	1,5	4	-	-	8	13,5	Р.6.1, № 2, гл. 1-4 Р.6.1, № 4, гл. 1,2 Р.6.2, № 2, гл. 1-4 Р.6.2, № 4, гл. 2-5 Р.6.2, № 7, гл. 1-4
4.2	STEM-системы, основные функции, архитектура, состав функциональных подсистем (модулей)	4	6	-	-	8	18	Р.6.1, № 5, гл. 4,5 Р.6.2, № 5, гл. 3 Р.6.2, № 8,9
4.3	Перспективы построения интеллектуальных систем комплексной оценки ИБ ИТКС	0,5	2	-	-	6	13,5	Р.6.1, № 2, гл. 4 Р.6.1, № 4, гл. 5 Р.6.2, № 5, гл.10-12

Занятия, проводимые в интерактивной форме, составляют 10% от общего количества аудиторных часов по дисциплине.

Лабораторные работы

№ занятия	№ раздела	Тема	Кол-во часов
1	3.1	Изучение функциональных возможностей программного комплекса оценки защищенности организаций MSAT	4
2	3.1	Применение программного комплекса MSAT для оценки уровня рисков информационной безопасности предприятия	4

Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1.2	Построение базовых моделей представления знаний предметной области (логические модели, семантические сети, фрейм-овые модели, продукционные правила)	2
2	2.1	Изучение основных положений Федеральных законов и руководящих документов ГТК (ФСТЭК) в области ИБ	2
3	2.2	Изучение основных положений международной системы стандартов и национальных стандартов в области ИБ	2
4	2.2	Нормативное закрепление базовых понятий ИБ (угрозы, уязвимости, риск) в стандартах и руководящих документах ФСТЭК	2
5	3.1	Понятие аудита ИБ, основные виды и формы проведения аудита ИБ	2
6	3.1	Международные методики проведения аудита ИБ (CRAMM, Risk Watch, MIST, OCTAVE и др.)	2
7	3.1	Инструментальные средства автоматизации процессов проведения аудита ИБ (КОНДОР, ГРИФ, MSAT и др.)	2
8	3.2	Сравнительный анализ достоинств и недостатков существующих методов и методик проведения аудита ИТСК. Тренды разработки систем автоматизации аудита ИБ	2
9	3.2	Нормативные документы ФСТЭК в области защиты ПДн	2
10	4.1	Архитектура и функции ЭС. Классификация ЭС, требования к методическому и информационному обеспечению ЭС	2
11	4.1	Основные этапы создания ЭС. Примеры построения ЭС в области комплексной оценки безопасности ИС	2
12	4.2	Архитектура и функции STEM-систем. Состав основных подсистем STEM, требования к этим подсистемам	2
13	4.2	Задачи, решаемые функциональными подсистемами STEM. Примеры реализации этих подсистем	2
14	4.2	Перспективы применения STEM-систем для решения задач мониторинга и контроля ИБ ИТКС	2
15	4.3	Интеллектуальные СППР по обеспечению безопасности ИТКС	2

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

6.1 Основная литература

1. Гузаиров М.Б. Управление защитой информации на основе интеллектуальных технологий [учеб. пособие для вузов] / М.Б. Гузаиров, И.В. Машкина. – М.: Машиностроение, 2013. – 241 с.
2. Юсупова Н.И. Интеллектуальная информационная поддержка принятия решений при анализе рисков чрезвычайных ситуаций и управлении ими / Н.И. Юсупова, К.Р. Еникеева. – Уфа: УГАТУ, 2014. – 206 с.
3. Михайлов Ю.Б. Научно-методические основы обеспечения безопасности защищаемых объектов. – М.: Горячая линия – Телеком, 2015. – 322 с.
4. Экспертные системы [учеб. пособие] / Н.И. Юсупова [и др.]. – Уфа: УГАТУ, 2014. – 89 с.

6.2 Дополнительная литература

1. Машкина И.В. Анализ риска объекта информатизации [учебн. пособие] / И.В. Машкина, Е.С. Степанова, Т.О. Вишнякова. – Уфа: УГАТУ, 2011. – 112 с.
2. Попов Д.В. Системы искусственного интеллекта. Эвристический поиск и инженерия знаний [учеб. пособие] / Д.В. Попов, Д.А. Ризванов. – Уфа: УГАТУ, 2012. – 117 с.
3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей [учеб. пособие]. – М.: Форум: Инфра – М., 2013. – 415 с.
4. Советов Б.Я. Интеллектуальные системы и технологии [учебник для вузов] / Б.Я. Советов, В.В. Цехановский, В.Д. Чертовской. – М.: Академия, 2013. – 320 с.
5. Васильев В. И. Искусственный интеллект: история в лицах [учеб. пособие]. – 2-е изд. – Уфа: УГАТУ, 2015. – 111 с.
6. Осипов Г.С. Лекции по искусственному интеллекту. – М.: ЛИБРОКОМ, 2014. – 272 с.
7. Джонс Т.М. Программирование искусственного интеллекта в приложениях / Пер. с англ. – М.: ДМК Пресс, 2015. – 312 с.
8. ГОСТ Р ИСО/МЭК 18045-2008 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».
9. ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска».

6.3. Интернет-ресурсы (электронные учебно-методические издания, лицензионное программное обеспечение)

На сайте библиотеки <http://library.ugatu.ac.ru/> в разделе «Информационные ресурсы», подраздел «Доступ к БД» размещены ссылки на интернет-ресурсы.

Обучающимся обеспечен доступ к электронным ресурсам и информационным справочным системам, перечисленным в таблице

Таблица

№	Наименование ресурса	Объем фонда электронных ресурсов	Доступ	Реквизиты договоров с правообладателям и
1.	ЭБС «Лань» http://e.lanbook.com/	41716	С любого компьютера, имеющего выход в	Договор № ЕД – 1185/0208-16 от 08.08.2016

			Интернет, после регистрации в ЭБС по сети УГАТУ	
2.	ЭБС Ассоциации «Электронное образование Республики Башкортостан» http://e-library.ufa-rb.ru	1225	С любого компьютера, имеющего выход в Интернет, после регистрации в АБИС «Руслан» на площадке библиотеки УГАТУ	Учредительный договор Ассоциации образовательных организаций «Электронное образование Республики Башкортостан» от 29.11.2013
3.	Консорциум аэрокосмических вузов России http://elsau.ru/	1235	С любого компьютера, имеющего выход в Интернет, после регистрации в АБИС «Руслан» на площадке библиотеки УГАТУ	Договор о сетевом взаимодействии от 15.12.2014
4.	Электронная коллекция образовательных ресурсов УГАТУ http://www.library.ugatu.ac.ru/cgi-bin/zgate.exe?Init+ugatu-fulltxt.xml,simple-fulltxt.xsl+rus	528	С любого компьютера по сети УГАТУ	Свидетельство о регистрац. №2012620618 от 22.06.2012
1.	Электронная библиотека диссертаций РГБ http://dvs.rsl.ru	885 898 экз.	Доступ с компьютеров читальных залов библиотеки, подключенных к ресурсу	Договор №2255/0208-15 от 23.12.2015
2.	База данных Proquest Dissertations and Theses Global http://search.proquest.com/	более 3,5 млн. диссертаций и дипломных работ	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и Государственной публичной научно-технической библиотекой России (далее ГПНТБ России) Сублиц. договор

				№ProQuest/151 52/0208-16 от 02.06.2016
3.	СПС «КонсультантПлюс»	2007691 экз.	По сети УГАТУ	Договор ЗК- 2318/0106-15 от 30.12.2015
4.	СПС «Гарант»	6139026 экз.	Доступ с компьютеров читальных залов библиотеки, подключенных к ресурсу	Договор 15\0208- 16 от 15.03.2016
5.	ИПС «Технорма/Документ»	36939 экз.	Локальная установка: библиотека УГАТУ-5 мест; кафедра стандартизации и метрологии- 1 место; кафедра начертательной геометрии и черчения-1 место	Договор № АОСС/914-15 № 989/0208-15 от 08.06.2015.
6.	Научная электронная библиотека eLIBRARY* http://elibrary.ru/	9919 полнотекстов ых журналов	С любого компьютера, имеющего выход в Интернет, после регистрации в НЭБ на площадке библиотеки УГАТУ	ООО «НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА». № 07-06/06 от 18.05.2006
7.	Патентная база данных компании Questel Orbit* http://www.orbit.com	55 млн. документов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №Questel/ 15146/0208-16 от 02.06.2016
8.	Научные полнотекстовые журналы издательства Taylor & Francis Group* http://www.tandfonline.com/	1700 наимен. журнал.	С любого компьютера по сети УГАТУ, имеющего выход в	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014

			Интернет	между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №Т&F/151 44/0208-16 от 02.06.2016
9.	Научные полнотекстовые журналы издательства Sage Publications* http://online.sagepub.com/	790 наимен. журнал.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №Sage/151 47/0208-16 от 02.06.2016
10.	Научные полнотекстовые журналы издательства Oxford University Press* http://www.oxfordjournals.org/	255 наимен. Журналов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №OUP-151 43/0208-16 от 02.06.2016
11.	База данных Computers & Applied Sciences Complete компании EBSCO Publishing http://search.ebscohost.com	1000 наим. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №CASC/151 50/0208-16 от 02.06.2016
12.	Научный полнотекстовый журнал Science The American	1 наимен. журнала.	С любого компьютера по	В рамках Государственного

	Association for the Advancement of Science http://www.sciencemag.org		сети УГАТУ, имеющего выход в Интернет	контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №Science/151 45/0208-16 от 02.06.2016
13.	Научные полнотекстовые журналы Американского института физики http://scitation.aip.org/	18 наимен. журналов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №AIP/151 48/0208-16 от 02.06.2016
14.	Научные полнотекстовые ресурсы Optical Society of America* http://www.opticsinfobase.org/	19 наимен. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №OSA/151 49/0208-16 от 02.06.2016
15.	База данных GreenFile компании EBSCO* http://www.greeninfoonline.com	5800 библиографич. записей, частично с полными текстами	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	Доступ предоставлен компанией EBSCO российским организациям-участникам консорциума НЭИКОН (в т.ч. УГАТУ - без подписания лицензионного договора)

16.	Реферативная база данных INSPEC компании EBSCO Publishing http://search.ebscohost.com	Более 11 млн. библиографич. записей		В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. Договор №INSPEC/151 51/0208-16 от 02.06.2016
17.	Архив научных полнотекстовых журналов зарубежных издательств* - http://archive.neicon.ru Annual Reviews (1936-2006) Cambridge University Press (1796-2011) цифровой архив журнала Nature (1869- 2011) Oxford University Press (1849–1995) SAGE Publications (1800-1998) цифровой архив журнала Science (1880 -1996) Taylor & Francis (1798-1997) Институт физики Великобритании The Institute of Physics (1874-2000)	2361 наимен. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	Доступ предоставлен российским организациям-участникам консорциума НЭИКОН (в т. ч. УГАТУ - без подписания лицензионного договора)

* Периодические издания получены по Гранту и на баланс библиотеки не принимались.

7. Методические указания по освоению дисциплины

Формы работы студентов: лекционные задания, практические занятия, написание рефератов, решение кейс-задач.

Дисциплина «Экспертные системы оценки безопасности информационно-телекоммуникационных систем» разбита на ряд отделов (модулей), представляющих собой логически завершенные части курса и являющихся теми комплексами знаний и умений, которые подлежат контролю.

Для оценки степени усвоения дисциплины рекомендуется проведение типовое задание и тестирование студентов по материалам лекций. Подборка вопросов для контрольных работ и тестирования осуществляется на основе изученного теоретического материала (см. раздел 6 настоящей рабочей программы).

В качестве организованной самостоятельной работы студентов рекомендуется использовать написания ими рефератов по выбранной тематике (см. раздел 4 рабочей программы). При написании реферата студент должен в соответствии с требованиями к оформлению работ, сформулировать проблему, актуальность, поставить цель и задачи исследования, сделать самостоятельный вывод о состоянии и путях решения данной проблемы.

9. Материально-техническое обеспечение дисциплины

Перечень лекционных аудиторий с современными средствами демонстрации: 5-301, 5-314, 5-317.

Перечень лабораторий современного, высокотехнологичного оборудования, обеспечивающего реализацию ОПОП ВО с учетом направленности подготовки:

- 5-317 – лаборатория ИТ и систем защиты информации;
- 5-418 – лаборатория технических средств защиты информации.

Вычислительное и телекоммуникационное оборудование и программные средства, необходимых для реализации ОПОП ВО и обеспечения физического доступа к информационным сетям, используемым в образовательном процессе и научно-исследовательской деятельности:

- компьютерная техника:
 - Intel Core i7-4790/ASUS Z97-K DDR3 ATX SATA3/Kingston DDR-III 2x4Gb 1600MHz/Segate 1Tb SATA-III/ Kingston SSD Disk 240Gb; серверы: CPU Intel Xenon E3-1240 V3 3.4GHz/4core/1+8Mb/80W/5GT ASUS P9D-C /4L LGA1150 / PCI-E SVGA 4xGbLAN SATA ATX 4DDR-III HDD 3 Tb SATA 6Gb/s Seagate Constellation CS 3,5” 7200rpm 64 Mb Crucia <CT102472BD160B> DDR-III DIMM 2x8Gb <ST3000NC002> CL11;
- программное обеспечение:
 - Программный комплекс – операционная система Microsoft Windows (№ договора ЭА-269/0503-16 , 1800 компьютеров, на которые распространяется право пользования)
 - Программный комплекс – Microsoft Office (№ договора ЭА-269/0503-16 , 1800 компьютеров, на которые распространяется право пользования)
 - Программный комплекс – Microsoft Project Professional (№ договора ЭА-269/0503-16 , 50 компьютеров, на которые распространяется право пользования)
 - Программный комплекс – операционная система Microsoft Visio Pro (№ договора ЭА-269/0503-16 , 50 компьютеров, на которые распространяется право пользования)
 - Kaspersky Endpoint Security для бизнеса (лицензии 1055/0503-16, 500 users).
 - Dr.Web® Desktop Security Suite (K3) +ЦУ (АН99-VCUN-TPPJ-6k3L, 415 рабочих станций).
 - ESET Smart Security Business (EAV-8424791, 500 пользователей).
 - Контур информационной безопасности SearchInform (UEI-2349-87, 25 пользователей).
 - Secret Net (IEK-109869, 25пользователей).
 - InfoWatch Traffic Monitor Enterprise (IWES-S3-DE, 25пользователей).
 - Seagate Central Discovery для ОС Windows (WOS-65-GT5, 25пользователей).

10. Адаптация рабочей программы для лиц с ОВЗ

При обучении инвалидов и лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата, обеспечивается возможность беспрепятственного доступа в учебные помещения и пункты питания и другие, необходимые для жизнедеятельности помещения, оборудованные пандусами, лифтами и иными средствами, облегчающими процесс передвижения. Для лиц с ограниченными возможностями здоровья по зрению предусматривается возможность доступа к зданию с собакой-поводырем.

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.