МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования «Вятский государственный университет»
(ВятГУ)
г. Киров

Утверждаю
Директор/Декан *Репкин Д. А.*

Номер регистрации
РПД_3-09.04.02.01_2021_116110
Актуализировано: 10.06.2021

Рабочая программа дисциплины
Кибербезопасность

наименование дисциплины

Квалификация выпускника	Магистр
Направление подготовки	09.04.02 шифр
	Информационные системы и технологии наименование
Направленность (профиль)	3-09.04.02.01 шифр
	Информационные технологии моделирования, анализа данных и принятия решений в управлении и экономике наименование
Формы обучения	Очная наименование
Кафедра-разработчик	Кафедра радиоэлектронных средств (ОРУ) наименование
Выпускающая кафедра	Кафедра систем автоматизации управления (ОРУ) наименование

Киров, 2021 г.

Сведения о разработчиках рабочей программы дисциплины

Трубин Игорь Сергеевич

ФИО

Цели и задачи дисциплины

Цель дисциплины	Целью преподавания дисциплины является формирование у обучающихся необходимых знаний, умений и навыков в области кибербезопасности в системах автоматизации управления производством (АСУП)
Задачи дисциплины	К основным задачам курса относятся: - знакомство со структурой государственной системы обеспечения информационной безопасности и основными стандартами по управлению информационной безопасностью - изучение теоретических, методологических и практических проблем в области кибербезопасности систем автоматизации управления производством; - приобретение практических навыков работы с нормативно-правовыми документами в области обеспечения защиты объектов КИИ; - формирование навыков принятия стратегических решений по обеспечению информационной безопасности в ходе планирования жизненного цикла информационных систем и АСУП.

Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Компетенция ПК-1

способен осуществлять планирование и оптимизацию развития сети связи и передачи данных		
Знает	Умеет	Владеет
средства сбора и анализа исходных данных для обеспечения требований информационной безопасности; действующие правовую и нормативную документацию, стандарты и технические условия в области информационной безопасности, защищенной связи и передачи данных; современные методы и подходы к формированию планов развития защищенной сети связи и передачи данных	использовать в работе современные информационные технологии обеспечения информационной безопасности, защищенной связи и передачи данных; анализировать новые средства связи с целью оценки соответствия техническим регламентам, международным и национальным стандартам в области информационной безопасности; использовать нормативную документацию в области инфокоммуникационных технологий и информационной безопасности	навыками формирования стратегических решений по обеспечению информационной безопасности в ходе планирования жизненного цикла информационных систем и сетей связи

Компетенция ПК-2

способен управлять этапами жизненного цикла методологической и технологической инфраструктуры анализа больших данных		
Знает	Умеет	Владеет
правовые основы работы с данными; методы, технологии и программное обеспечение систем хранения, передачи и обработки информации; методы управления информационными ресурсами организации; методы и средства управления информационной безопасностью; принципы обеспечения безопасности в распределенных информационных системах производственного и административного назначения; принципы анализа потребностей в работе с большими данными и формирования заданий, проектов и планов на их основе	анализировать потребности в работе с большими данными и сопутствующие им требования; разрабатывать проекты информационно-технологической инфраструктуры организации и управлять их реализацией; разрабатывать и согласовывать проектную и эксплуатационную документацию информационно-технологических проектов; формировать стратегию развития методологической и технологической инфраструктуры анализа больших данных	разработки и реализации процесса управления информационной безопасностью и обеспечением конфиденциальности при анализе больших данных

Компетенция ПК-3

способен организовывать проведение работ по проектированию автоматизированных систем управления производством		
Знает	Умеет	Владеет
виды объектов и категорий критической информационной инфраструктуры; методы и средства защиты объектов критической информационной инфраструктуры	применять нормативную документацию в области обеспечения безопасности критической информационной инфраструктуры	навыками категорирования, определения угроз и выбора методов и средств защиты критической информационной инфраструктуры

Структура дисциплины

Тематический план

№ п/п	Наименование разделов дисциплины	Шифр формируемых компетенций
1	Нормативно-правовая база в области кибербезопасности	ПК-1
2	Принципы обеспечения безопасности в распределенных информационных системах	ПК-2
3	Методы и средства защиты критической информационной инфраструктуры	ПК-3
4	Подготовка и прохождение промежуточной аттестации	ПК-1, ПК-2, ПК-3

Формы промежуточной аттестации

Зачет	3 семестр (Очная форма обучения)
Экзамен	Не предусмотрен (Очная форма обучения)
Курсовая работа	Не предусмотрена (Очная форма обучения)
Курсовой проект	Не предусмотрена (Очная форма обучения)

Трудоемкость дисциплины

Форма обучения	Курсы	Семестры	Общий объем (трудоемкость)		Контактная работа, час	в том числе аудиторная контактная работа обучающихся с преподавателем, час				Самостоятельная работа, час	Курсовая работа (проект), семестр	Зачет, семестр	Экзамен, семестр
			Часов	ЗЕТ		Всего	Лекции	Семинарские, практические занятия	Лабораторные занятия				
Очная форма обучения	2	3	144	4	79.5	32	16	16	0	64.5		3	

Содержание дисциплины

Очная форма обучения

Код занятия	Наименование тем занятий	Трудоемкость, академических часов
Раздел 1 «Нормативно-правовая база в области кибербезопасности»		**25.00**
Лекции		
Л1.1	Структура государственной системы обеспечения информационной безопасности	1.00
Л1.2	Структура и основные направления развития нормативно-правовой базы в области информационной безопасности	1.00
Л1.3	Стандарты в области обеспечения информационной безопасности	1.00
Семинары, практические занятия		
П1.1	Серия стандартов ISO/IEC 27000 "Информационные технологии. Методы обеспечения безопасности"	2.00
Самостоятельная работа		
С1.1	Содержание основных законов Российской Федерации в области информационной безопасности (проработка материалов лекции Л1.1)	2.00
С1.2	Основные руководящие нормативно-технические, методические и организационные документы в области информационной безопасности (проработка материалов лекции Л.1.2)	6.00
С1.3	Серия стандартов ISO/IEC 27000 "Информационные технологии. Методы обеспечения безопасности" (подготовка к практическому занятию П1.3)	2.00
Контактная внеаудиторная работа		
КВР1.1	Контактная внеаудиторная работа	10.00
Раздел 2 «Принципы обеспечения безопасности в распределенных информационных системах»		**59.00**
Лекции		
Л2.1	ИС как среда для обработки, хранения и передачи информации. Жизненный цикл ИС	1.00
Л2.2	Жизненный цикл типовой информационной атаки на ресурсы ИС	1.00
Л2.3	Распределение механизмов и услуг безопасности по уровням архитектуры ЭМВОС	2.00
Л2.4	Управление и система управления информационной безопасности	1.00
Л2.5	Понятие политики информационной безопасности организации	1.00
Семинары, практические занятия		
П2.1	Разработка политики информационной безопасности	2.00
П2.2	Метрики защиты CVSS (Common Vulnerability Scoring	2.00

	System)	
П2.3	Изучение структуры InfoWatch TM и DM	2.00
П2.4	Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	2.00
Самостоятельная работа		
С2.1	Архитектура безопасности ЭМВОС (проработка материалов лекции Л2.1 - Л2.3)	2.00
С2.2	Изучение документации InfoWatch TM (подготовка к практическим занятиям П2.3 - П2.4)	10.00
С2.3	Методика расчета метрик CVSS 2.0 и 3.0 (проработка материалов лекции Л2.3, подготовка к практике П2.2)	3.00
С2.4	Стадии жизненного цикла информационной атаки на ресурсы ИС (проработка материалов лекции Л2.2)	2.00
С2.5	Изучение примеров частных политик информационной безопасности (подготовка к практическому занятию П2.1)	6.00
С2.6	Система управления информационной безопасностью организации (проработка материалов лекции Л2.4)	2.00
Контактная внеаудиторная работа		
КВР2.1	Контактная внеаудиторная работа	20.00
Раздел 3 «Методы и средства защиты критической информационной инфраструктуры»		**56.00**
Лекции		
Л3.1	Правовой режим обеспечения информационной безопасности объектов КИИ	2.00
Л3.2	Система защиты информации как основа безопасного функционирования АС	2.00
Л3.3	Базовые технологии обеспечения информационной безопасности	3.00
Семинары, практические занятия		
П3.1	Категорирование объектов КИИ	2.00
П3.2	Методика определения актуальных угроз безопасности персональных данных при их обработке в ИСПДН	2.00
П3.3	Оформление технического (частного технического) задания на разработку системы (подсистемы) защиты объектов КИИ	2.00
Самостоятельная работа		
С3.1	Законодательная и нормативная база правового регулирования вопросов защиты КИИ. Руководящие документы по защите КИИ (подготовка к практическим занятиям П3.1 - П3.3))	8.00
С3.2	Основы аутентификации (проработка материалов лекции Л3.3)	4.00
С3.3	Технология межсетевого экранирования (проработка материалов лекции Л3.3)	4.00
С3.4	Концепция обеспечения ИБ (проработка материалов лекций Л3.1 - Л3.2)	2.00

С3.5	Средства обеспечения ИБ (проработка материалов лекции Л3.2)	2.00
С3.6	Службы обеспечения информационной безопасности (проработка материалов лекции Л3.2)	2.00
С3.7	Участники обеспечения ИБ (проработка материалов лекции Л3.2)	2.00
С3.8	Основные функции СЗИ (проработка материалов лекции Л3.2)	2.00
Контактная внеаудиторная работа		
КВР3.1	Контактная внеаудиторная работа	17.00
Раздел 4 «Подготовка и прохождение промежуточной аттестации»		**4.00**
34.1	Подготовка к сдаче зачета	3.50
КВР4.1	Сдача зачета	0.50
ИТОГО		**144.00**

Содержание дисциплины данной рабочей программы используется при обучении по индивидуальному учебному плану, при ускоренном обучении, при применении дистанционных образовательных технологий и электронном обучении (при наличии).

Методические указания для обучающихся по освоению дисциплины

Успешное освоение дисциплины предполагает активное, творческое участие обучающегося на всех этапах ее освоения путем планомерной, повседневной работы. Обучающийся обязан посещать лекции, семинарские, практические и лабораторные занятия (при их наличии), получать консультации преподавателя и выполнять самостоятельную работу.

Изучение дисциплины следует начинать с проработки настоящей рабочей программы, методических указаний и разработок, указанных в программе, особое внимание уделить целям, задачам, структуре и содержанию дисциплины.

Главной задачей каждой лекции является раскрытие сущности темы и анализ ее основных положений. Тематика лекций определяется настоящей рабочей программой дисциплины.

Лекции – это систематическое устное изложение учебного материала. На них обучающийся получает основной объем информации по каждой конкретной теме. Лекции обычно носят проблемный характер и нацелены на освещение наиболее трудных и дискуссионных вопросов.

Предполагается, что обучающиеся приходят на лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендованным программой. Часто обучающимся трудно разобраться с дискуссионными вопросами, дать однозначный ответ. Преподаватель, сравнивая различные точки зрения, излагает свой взгляд и нацеливает их на дальнейшие исследования и поиск научных решений. После лекции желательно вечером перечитать и закрепить полученную информацию, тогда эффективность ее усвоения значительно возрастает. При работе с конспектом лекции необходимо отметить материал, который вызывает затруднения для понимания, попытаться найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь за помощью к преподавателю.

Целью семинарских занятий является проверка уровня понимания обучающимися вопросов, рассмотренных на лекциях и в учебной литературе.

Целью практических и лабораторных занятий является формирование у обучающихся умений и навыков применения теоретических знаний в реальной практике решения задач; восполнение пробелов в пройденной теоретической части курса.

Семинарские, практические и лабораторные занятия в равной мере направлены на совершенствование индивидуальных навыков решения теоретических и прикладных задач, выработку навыков интеллектуальной работы, а также ведения дискуссий. Для успешного участия в семинарских, практических и лабораторных занятиях обучающемуся следует тщательно подготовиться.

Основной формой подготовки обучающихся к практическим (лабораторным) занятиям является самостоятельная работа с учебно-методическими материалами, научной литературой, статистическими данными и т.п.

Изучив конкретную тему, обучающийся может определить, насколько хорошо он в ней разобрался. Если какие-то моменты остались непонятными, целесообразно составить список вопросов и на занятии задать их преподавателю. Практические (лабораторные) занятия предоставляют обучающемуся возможность творчески раскрыться, проявить инициативу и развить навыки публичного ведения дискуссий и общения.

Самостоятельная работа обучающихся включает в себя выполнение различного рода заданий (изучение учебной и научной литературы, материалов лекций, систематизацию прочитанного материала, подготовку контрольной работы, решение

задач, подготовка докладов, написание рефератов, публикация тезисов, научных статей, подготовка и защита курсовой работы / проекта и другие), которые ориентированы на глубокое усвоение материала изучаемой дисциплины.

Обучающимся рекомендуется систематически отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки.

Внутренняя система оценки качества освоения дисциплины включает входной контроль уровня подготовленности обучающихся, текущий контроль успеваемости, промежуточную аттестацию, направленную на оценивание промежуточных и окончательных результатов обучения по дисциплине (в том числе результатов курсового проектирования (выполнения курсовых работ) при наличии).

При проведении промежуточной аттестации обучающегося учитываются результаты текущего контроля, проводимого в течение освоения дисциплины.

Процедура оценивания результатов освоения дисциплины осуществляется на основе действующих локальных нормативных актов ФГБОУ ВО «Вятский государственный университет», с которыми обучающиеся ознакамливаются на официальном сайте университета www.vyatsu.ru.

Учебно-методическое обеспечение дисциплины, в том числе учебно-методическое обеспечение самостоятельной работы обучающегося по дисциплине

Учебная литература (основная)

1) Словарь-справочник терминов в области кибербезопасности / М-во образования и науки РФ, Центр информ. технологий и систем органов исполн. власти ; [авт.-сост. И. М. Воронков и др.]. - Москва : Сам полиграфист, 2014. - 232 с. : табл. ; 25 см. - Библиогр.: с. 219-221, 225-228. - 300 экз. - ISBN 978-5-00077-165-5 : 350.00 р. - Текст : непосредственный.

5) Организационное и правовое обеспечение информационной безопасности : учебник и практикум / под ред. Т. А. Поляковой, А. А. Стрельцова. - Москва : Юрайт, 2017. - 324 с. - (Бакалавр. Магистр). - Библиогр.: с. 324-325. - ISBN 978-5-534-03600-8 : 779.00 р. - Текст : непосредственный.

3) Милославская, Наталья Георгиевна. Технические, организационные и кадровые аспекты управления информационной безопасностью : учеб. пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - Москва : Горячая линия-Телеком, 2012. - 214 с. - (Вопросы управления информационной безопасностью ; вып. 4). - Библиогр.: с. 209-211. - ISBN 978-5-9912-0274-9 : 392.70 р. - Текст : непосредственный.

4) Основы управления информационной безопасностью : учебное пособие для вузов / А.П. Курило. - Москва : Горячая линия - Телеком, 2013. - 244 с. - (Вопросы управления информационной безопасностью. Вып. 1). - ISBN 978-5-9912-0271-8 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=253575/ (дата обращения: 03.03.2021). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

2) Шилов, А. К. Управление информационной безопасностью : учебное пособие / А.К. Шилов. - Ростов-на-Дону|Таганрог : Южный федеральный университет, 2018. - 121 с. : ил. - Библиогр.: с. 81-82. - ISBN 978-5-9275-2742-7 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=500065/ (дата обращения: 03.03.2021). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

6) Гультяева, Т. А. Основы информационной безопасности : учебное пособие / Т.А. Гультяева. - Новосибирск : Новосибирский государственный технический университет, 2018. - 79 с. : ил., табл. - Библиогр. в кн. - ISBN 978-5-7782-3640-0 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=574729/ (дата обращения: 03.03.2021). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

Учебная литература (дополнительная)

1) Кибербезопасность в условиях электронного банкинга : практическое пособие / А. А. Бердюгин, А. Б. Дудка, С. В. Конявская, В. А. Конявский, И. Г. Назаров. -

Москва : Прометей, 2020. - 522 с. : ил. - Библиогр. в кн. - ISBN 978-5-907244-61-0 : Б. ц. - URL: https://biblioclub.ru/index.php?page=book&id=610688/ (дата обращения: 03.03.2021). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

2) Анализ состояния защиты данных в информационных системах : учебно-методическое пособие. - Новосибирск : НГТУ, 2012. - 52 с. - ISBN 978-5-7782-1969-4 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=228844/ (дата обращения: 03.03.2021). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

3) Нестеров, С. А. Основы информационной безопасности : учебное пособие / С.А. Нестеров. - Санкт-Петербург : Издательство Политехнического университета, 2014. - 322 с. - ISBN 978-5-7422-4331-1 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=363040/ (дата обращения: 03.03.2021). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

4) Балановская, Анна Вячеславовна. Организационно-экономические механизмы обеспечения эффективности управления информационной безопасностью промышленных предприятий : монография / А. В. Балановская, А. В. Волкодаева ; Администрация гор. округа Самара, Самар. акад. гос. и муницип. упр. - Самара : Изд-во САГМУ, 2012. - 248 с. - Библиогр.: с. 231-246. - ISBN 978-5-94189-117-7 : 180.00 р. - Текст : непосредственный.

5) Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. - 284 с. - Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=480637/ (дата обращения: 03.03.2021). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

6) Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Издательство «Флинта», 2016. - 224 с. - (Организация и технология защиты информации). - Библиогр.: с. 192-193. - ISBN 978-5-9765-1274-0 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=93351/ (дата обращения: 03.03.2021). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

Периодические издания

1) Телекоммуникации . - М. : ООО "Наука и технологии", 2000 - . - Загл. с титул. экрана. - Электрон. версия печ. публикации . - Выходит ежемесячно - URL: http://elibrary.ru/title_about.asp?id=9147. - Режим доступа: Научная электронная библиотека eLIBRARY.RU.. - Текст : электронный.

2) Современные технологии автоматизации . - М. : ООО "СТА-ПРЕСС", 1996 - . - Выходит ежеквартально. - ISSN 0206-975X. - Текст : непосредственный.

3) Инфокоммуникационные технологии : период. науч.-техн. и информац.-аналит. журн.. - Самара : Поволжская государственная академия телекоммуникаций и информатики, 2003 - . - Выходит ежеквартально. - ISSN 2037-3909. - Текст : непосредственный.

4) Проблемы информационной безопасности. Компьютерные системы. - СПб. : [б. и.], 1999 - . - Выходит ежеквартально. - ISSN 2071-8217. - Текст : непосредственный.

Электронные образовательные ресурсы

1) Портал дистанционного обучения ВятГУ [электронный ресурс] / - Режим доступа: http://mooc.do-kirov.ru/
2) Раздел официального сайта ВятГУ, содержащий описание образовательной программы [электронный ресурс] / - Режим доступа: https://www.vyatsu.ru/php/programms/eduPrograms.php?Program_ID=3-09.04.02.01
3) Личный кабинет студента на официальном сайте ВятГУ [электронный ресурс] / - Режим доступа: https://new.vyatsu.ru/account/
4) Единое окно доступа к образовательным ресурсам http://window.edu.ru/

Электронные библиотечные системы (ЭБС)

- ЭБС «Научная электронная библиотека eLIBRARY» (http://elibrary.ru/defaultx.asp)
- ЭБС «Издательства Лань» (http://e.lanbook.com/)
- ЭБС «Университетская библиотека online» (www.biblioclub.ru)
- Внутренняя электронно-библиотечная система ВятГУ (http://lib.vyatsu.ru/)
- ЭБС «ЮРАЙТ (https://urait.ru)

Современные профессиональные базы данных и информационные справочные системы

- ГАРАНТ
- КонсультантПлюс
- Техэксперт: Нормы, правила, стандарты
- Роспатент (https://www1.fips.ru/elektronnye-servisy/informatsionno-poiskovaya-sistema)
- Web of Science® (http://webofscience.com)

Материально-техническое обеспечение дисциплины

Демонстрационное оборудование

Перечень используемого оборудования
ИНТЕРАКТИВНАЯ ДОСКА SMART BOARD 480IV СО ВСТРОЕННЫМ ПРОЕКТОРОМ V25 С КАБЕЛЕМ VGA 15,2М C-GM/GM-50
ПРОЕКТОР Acer P5260a DLP 1024x768. 3.0KG.2000:1 2700 LUME
ЭКРАН настенный Manual 240 x240см

Специализированное оборудование

Перечень используемого оборудования
КОММУТАТОР Catalyst 2960 24
МАРШРУТИЗАТОР C1921
МАРШРУТИЗАТОР Cisco 2901
МЕЖСЕТЕВОЙ ЭКРАН Cisco ASA 5505
ПЕРСОНАЛЬНЫЙ КОМПЬЮТЕР ICL SafeRay S251.Mi (МОНОБЛОК)
РАБОЧАЯ СТАНЦИЯ ТЕЛЕКОММУНИКАЦИОННОГО ДОСТУПА К КЛАСТЕРНОЙ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЕ И ХРАНИЛИЩУ ДАННЫХ
ТОЧКА БЕСПРОВОДНОГО ДОСТУПА ЛВС Cisco AIRONET 1600
ШКАФ ТЕЛЕКОММУНИКАЦИОННЫЙ НАПОЛЬНЫЙ 19" (600x1020x2030)

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе лицензионное и свободно распространяемое ПО (включая ПО отечественного производства)

№ п.п	Наименование ПО	Краткая характеристика назначения ПО
1	Программная система с модулями для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ»	Программный комплекс для проверки текстов на предмет заимствования из Интернет-источников, в коллекции диссертация и авторефератов Российской государственной библиотеки (РГБ) и коллекции нормативно-правовой документации LEXPRO
2	Microsoft Office 365 ProPlusEdu ALNG SubsVL MVL AddOn toOPP	Набор веб-сервисов, предоставляющий доступ к различным программам и услугам на основе платформы Microsoft Office, электронной почте бизнес-класса, функционалу для общения и управления документами
3	Office Professional Plus 2016	Пакет приложений для работы с различными типами документов: текстами, электронными таблицами, базами данных, презентациями
4	Windows Professional	Операционная система
5	Kaspersky Endpoint Security для бизнеса	Антивирусное программное обеспечение
6	Справочная правовая система «Консультант Плюс»	Справочно-правовая система по законодательству Российской Федерации
7	Электронный периодический справочник ГАРАНТ Аналитик	Справочно-правовая система по законодательству Российской Федерации
8	Security Essentials (Защитник Windows)	Защита в режиме реального времени от шпионского программного обеспечения, вирусов.
9	МойОфис Стандартный	Набор приложений для работы с документами, почтой, календарями и контактами на компьютерах и веб браузерах
10	2019 ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ InfoWatch Traffic Monitor Education Lab Extended бессрочная лицензия на 16 серверов	Специализированное лицензионное ПО

Обновленный список программного обеспечения данной рабочей программы находится по адресу: https://www.vyatsu.ru/php/list_it/index.php?op_id=116110