

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сыров Игорь Анатольевич
Должность: Директор
Дата подписания: 30.10.2023 11:12:34
Уникальный программный ключ:
b683afe664d7e9f64175886cf9626a196149ad36

СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет Математики и информационных технологий
Кафедра Математического моделирования

Рабочая программа дисциплины (модуля)

дисциплина ***Б1.О.17 Методы и средства защиты информации***

обязательная часть

Направление

09.03.03 ***Прикладная информатика***
код наименование направления

Программа

Мобильные и сетевые технологии

Форма обучения

Заочная

Для поступивших на обучение в
2023 г.

Разработчик (составитель)
к.ф.-м.н., доцент
Викторов С. В.
ученая степень, должность, ФИО

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций	3
2. Цели и место дисциплины (модуля) в структуре образовательной программы	4
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся	5
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий.....	5
4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах).....	5
4.2. Содержание дисциплины, структурированное по разделам (темам)	6
5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю).....	7
6. Учебно-методическое и информационное обеспечение дисциплины (модуля)	11
6.1. Перечень учебной литературы, необходимой для освоения дисциплины (модуля)	11
6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем	11
6.3. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства	15
7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)	15

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)
ОПК-2. Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности;	ОПК-2.1. Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.	Обучающийся должен: знать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.
	ОПК-2.2. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.	Обучающийся должен: уметь выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.
	ОПК-2.3. Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	Обучающийся должен: владеть навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.
ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;	ОПК-4.1. Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Обучающийся должен: знать основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
	ОПК-4.2. Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Обучающийся должен: уметь применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.

	ОПК-4.3. Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы.	Обучающийся должен: владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы.
ОПК-5. Способен установить программное и аппаратное обеспечение для информационных и автоматизированных систем;	ОПК-5.1. Знает основы системного администрирования, администрирования СУБД, современные стандарты информационного взаимодействия систем.	Обучающийся должен: знать основы системного администрирования, администрирования СУБД, современные стандарты информационного взаимодействия систем.
	ОПК-5.2. Умеет выполнять параметрическую настройку информационных и автоматизированных систем	Обучающийся должен: уметь выполнять параметрическую настройку информационных и автоматизированных систем
	ОПК-5.3. Владеет навыками установки программного и аппаратного обеспечения информационных и автоматизированных систем	Обучающийся должен: владеть навыками установки программного и аппаратного обеспечения информационных и автоматизированных систем

2. Цели и место дисциплины (модуля) в структуре образовательной программы

Цели изучения дисциплины:

Дисциплина «Методы и средства защиты информации» является дисциплиной, дающей начальные представления и понятия в области информационной безопасности, определяющей потребности в развитии интереса к изучению учебных дисциплин и профессиональных модулей, способности к личному самоопределению и самореализации в учебной деятельности.

Основной задачей преподавания дисциплины является подготовка специалистов, обладающих знаниями, навыками, умениями в сфере обеспечения информационной безопасности организаций различных форм собственности.

Уровень освоения содержания дисциплины предполагает: - Знакомство с основными понятиями информационной безопасности, информационными угрозами, их классификацией, и возможными последствиями для организаций различных форм собственности; Уяснение вопросов обеспечения информационной безопасности организации и проблем создания (концептуального проектирования) систем информационной безопасности; - Принятие обоснованных решений по выбору политики информационной безопасности (ИБ) и оценки эффективности инвестиций в ИБ. Знания, навыки и умения, приобретенные в процессе изучения дисциплины в ходе лекций, практических занятий и самостоятельной работы, должны всесторонне использоваться студентами в процессе дальнейшей профессиональной деятельности при решении

широкого класса аналитических задач финансово-экономического характера. Дисциплина реализуется в рамках части, формируемой участниками образовательных отношений .

Дисциплина изучается на 4 курсе в 7, 8 семестрах

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 180 акад. ч.

Объем дисциплины	Всего часов
	Заочная форма обучения
Общая трудоемкость дисциплины	180
Учебных часов на контактную работу с преподавателем:	
лекций	6
практических (семинарских)	12
лабораторных	12
другие формы контактной работы (ФКР)	1,2
Учебных часов на контроль (включая часы подготовки):	7,8
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР)	141

Формы контроля	Семестры
экзамен	8

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

№ п/п	Наименование раздела / темы дисциплины	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
		Контактная работа с преподавателем			СР
		Лек	Пр/Сем	Лаб	
1	Криптография донаучного периода.	1	2	1	40
1.1	Донаучный период криптографии.	0	1	1	30
1.2	Основные криптографические примитивы.	1	1	0	10
2	Алгоритмы симметричного шифрования.	2	7	6	50
2.1	Требования к алгоритмам симметричного шифрования.	1	0	0	16

	Режимы выполнения.				
2.2	Алгоритмы симметричного шифрования ГОСТ и DES.	1	7	6	34
3	Алгоритмы асимметричного шифрования.	3	3	5	51
3.1	Требования к алгоритмам асимметричного шифрования Алгоритм RSA.	1	1	2	20
3.2	Хэш-функции.	1	1	1	15
3.3	Электронная цифровая подпись.	1	1	2	16
	Итого	6	12	12	141

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Криптография донаучного периода.	
1.2	Основные криптографические примитивы.	Подстановки. Перестановки. Гаммирование. Нелинейное преобразование с помощью S-боксов. Комбинированные методы.
2	Алгоритмы симметричного шифрования.	
2.1	Требования к алгоритмам симметричного шифрования. Режимы выполнения.	Криптография. Сеть Фейштеля. Криптоанализ. Используемые критерии при разработке алгоритмов симметричного шифрования. 4 режима выполнения.
2.2	Алгоритмы симметричного шифрования ГОСТ и DES.	Алгоритм DES. Алгоритм генерации ключей. Алгоритм ГОСТ 2814. Сравнительный анализ ГОСТ и DES. Создание случайных чисел.
3	Алгоритмы асимметричного шифрования.	
3.1	Требования к алгоритмам асимметричного шифрования Алгоритм RSA.	Основные требования к алгоритмам асимметричного шифрования. Математический аппарат алгоритма RSA.
3.2	Хэш-функции.	Требования к хэш-функциям. Простые хэш-функции. Сильные хэш- функции
3.3	Электронная цифровая подпись.	Требования к цифровой подписи. Прямая и арбитражная цифровые подписи.

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Криптография донаучного периода.	
1.1	Донаучный период криптографии.	Программирование алгоритма Гронсфельда.
2	Алгоритмы симметричного шифрования.	
2.2	Алгоритмы симметричного шифрования ГОСТ и DES.	Разработка приложения алгоритма ГОСТ (шифрование/дешифрование).
3	Алгоритмы асимметричного шифрования.	
3.1	Требования к алгоритмам асимметричного шифрования Алгоритм RSA.	Программирование алгоритма RSA.
3.2	Хэш-функции.	Создание хеш-образа сообщения с помощью хеш-функции цепочки зашифрованных блоков.

3.3	Электронная цифровая подпись.	Создание электронной цифровой подписи на основе RSA.
-----	-------------------------------	--

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Криптография донаучного периода.	
1.1	Донаучный период криптографии.	Разбор алгоритмов шифрования Цезаря, Гронефельда, Трипемуса, Бодо. Шифрование биграммами.
1.2	Основные криптографические примитивы.	Частотные характеристики открытых сообщений. Определение частотных характеристик криптограммы. Определение вероятностных характеристик алфавита.
2	Алгоритмы симметричного шифрования.	
2.2	Алгоритмы симметричного шифрования ГОСТ и DES.	Работа с S-box, кодовой таблицей. Выполнение алгоритма ГОСТ (2 раунда). Дешифрование ГОСТ. Разработка соответствующих процедур.
3	Алгоритмы асимметричного шифрования.	
3.1	Требования к алгоритмам асимметричного шифрования Алгоритм RSA.	Генерация открытого и закрытого ключей RSA. Шифрование и дешифрование.
3.2	Хэш-функции.	Изучение сильных хэш-функций MD4, MD5.
3.3	Электронная цифровая подпись.	Изучение стандарта цифровой подписи DSS и ГОСТ 3410.

5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю)

Методические указания для обучающихся по освоению дисциплины.

При изучении дисциплины необходимо обратить внимание на то, что составление плана работы производить кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометить важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий осуществляется с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе.

Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Уделить внимание следующим понятиям: информация, информационные технологии, эволюция ИТ, классификация ИТ, средства и методы ИТ, поколения ЭВМ, архитектура ЭВМ, внешние и внутренние устройства ПК, компьютерная сеть, программное обеспечение, операционная система, прикладное программное обеспечение, информатизация общества, информационная деятельность, информационная культура, понятие информационных и коммуникационных технологий, средств информационных и коммуникационных технологий, мультимедиа, технология телекоммуникации, электронные средства учебного назначения, электронные учебники, базы данных и базы

знаний, экспертные обучающие системы, интеллектуальные обучающие системы, образовательные порталы и сайты, электронный портфолио, дистанционное обучение и др.

При выполнении и защите практических работ следует руководствоваться учебно-методическими указаниями преподавателя и рекомендованными практикумами, которые отражают технологическую составляющую дисциплины. Они помогут получить навыки работы на персональном компьютере в программных продуктах, изучение которых предусмотрено программой. Практикумы можно использовать как самоучители, с помощью которых можно самостоятельно освоить базовые компьютерные технологии.

Изучение практикумов принесет максимальную пользу, если учащиеся будут читать его, одновременно выполняя предлагаемые в книгах задания. Благодаря такой методике начинают действовать средства самоконтроля: инструментарий программной среды осваивается не просто в процессе чтения, а в ходе решения практических задач. Рекомендуется сначала выполнить простые задания для освоения базовой (типовой) технологии. По мере освоения программной среды ставятся все более сложные задачи, при решении которых будут активизироваться знания дополнительных возможностей данной среды. Итак, переходя от простых заданий к более сложным, будет освоена большая часть технологических операций в конкретной программной среде и достигнут достаточно высокий профессиональный уровень. Сдача и защита контрольной работы включает проверку электронных файлов и ответы на контрольные вопросы, которые должны продемонстрировать теоретические и практические знания, умения и навыки по соответствующей теме.

№ п/п	Тема и содержание	Задания по самостоятельной работе студентов	
		СР	
1	2	6	8
1.	Криптография донаучного периода	40	
1.1.	Донаучный период криптографии.	30	подготовка к индивидуальному опросу; подготовка к практическим работам; подготовка к контрольной работе;
1.2.	Основные криптографические примитивы	10	подготовка к индивидуальному опросу; подготовка к практическим работам; подготовка к контрольной работе;

2.	Алгоритмы симметричного шифрования	50	
2.1.	Требования к алгоритмам симметричного шифрования. Режимы выполнения.	16	подготовка к индивидуальному опросу; подготовка к практическим работам;
2.2.	Алгоритмы симметричного шифрования ГОСТ и DES	34	подготовка к индивидуальному опросу; подготовка к практическим работам; подготовка к тестированию;
3.	Алгоритмы асимметричного шифрования.	51	
3.1.	Требования к алгоритмам асимметричного шифрования Алгоритм RSA.	20	подготовка к индивидуальному опросу; подготовка к практическим работам;
3.2.	Хэш-функции	15	подготовка к индивидуальному опросу; подготовка к практическим работам; подготовка к тестированию;
3.3.	Электронная цифровая подпись	16	подготовка к практическим работам; подготовка к тестированию;
	Всего часов:	141	

Внеаудиторными формами и инструментами самостоятельной работы студентов по дисциплине являются: работа с конспектом лекций, изучение дополнительного теоретического материала, подготовка к занятиям, тестированию/контрольной работе.

Наименование тем на самостоятельное изучение:

1. Информационные войны и информационное противоборство.
2. Определение и основные виды информационных войн
3. Информационно-техническая война.
4. Информационно-психологическая война.

Вопросы для самоконтроля

1. Чем отличаются понятия «информационная война» и «информационное противоборство»?
2. Чем отличается информационная война от обычного вооруженного конфликта?
3. Какие виды информационных войн Вы можете выделить?
4. Приведите пример межкорпоративной информационной войны.
5. Можно ли рассматривать рекламу как средство ведения информационной борьбы?
6. Какие приемы ведения информационной войны используются во время предвыборных кампаний, приведите примеры.
7. Что такое информационное оружие? Какие виды оружия применяются в ходе ведения информационной войны?
8. Каковы цели информационной войны?
9. Каковы средства и методы защиты от информационно-технического оружия?
10. Каковы особенности информационно-психологической войны?

Рекомендуемая учебно-методическая литература:

1. Новиков, В. К. Организационно-правовые основы информационной безопасности (защиты информации): юридическая ответственность за правонарушения : учебное пособие / В. К. Новиков. – Москва : Горячая линия – Телеком, 2015. – 175 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=457171>.
2. Основы управления информационной безопасностью: учебное пособие для вузов / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Москва : Горячая линия – Телеком, 2013. – 244 с. : ил. – (Вопросы управления информационной безопасностью. Вып. 1). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=253575> .
3. Беляков, С. Л. Основы разработки программ на языке C++ для систем информационной безопасности : учебное пособие : [16+] / С. Л. Беляков, А. В. Боженюк, М. В. Петряева ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – 152 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=612164> .
4. Сычев, Ю. Н. Основы информационной безопасности: учебно-практическое пособие : учебное пособие / Ю. Н. Сычев. – Москва : Евразийский открытый институт, 2010. – 328 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=90790> .
5. Галатенко, В. А. Основы информационной безопасности: Курс лекций : учебное пособие / В. А. Галатенко ; под ред. В. Б. Бетелина. – Изд. 3-е. – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2006. – 208 с. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=233063> .

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

6.1. Перечень учебной литературы, необходимой для освоения дисциплины (модуля)

Основная учебная литература:

1. Бирюков, А.А. Информационная безопасность: защита и нападение. [Электронный ресурс] : учебник. — Электрон. дан. — М. : ДМК Пресс, 2012. — 474 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=39990 (26.06.2023).
2. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ДМК Пресс, 2014. — 702 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=50578 (26.06.2023).
3. Чечёта, С.И. Введение в дискретную теорию информации и кодирования : учебное пособие / С.И. Чечёта. - Москва : МЦНМО, 2011. - 224 с. : табл., схем. - ISBN 978-5-94057-701-0 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=63307> (26.06.2023).

Дополнительная учебная литература:

1. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] : . — Электрон. дан. — М. : ДМК Пресс, 2008. — 448 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=3027 (26.06.2023).
2. Галатенко, В.А. Основы информационной безопасности / В.А. Галатенко. - Изд. 3-е. - М. : Интернет-Университет Информационных Технологий, 2006. - 208 с. - (Основы информационных технологий). - ISBN 5-9556-0052-3 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=233063> (26.06.2023).
3. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=363040> (26.06.2023).

6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем

№ п/п	Наименование документа с указанием реквизитов
1	Договор на доступ к ЭБС ZNANIUM.COM между БашГУ в лице директора СФ БашГУ и ООО «Знаниум» № 3/22-эбс от 05.07.2022
2	Договор на доступ к ЭБС «ЭБС ЮРАЙТ» (полная коллекция) между БашГУ в лице директора СФ БашГУ и ООО «Электронное издательство ЮРАЙТ» № 1/22-эбс от 04.03.2022
3	Договор на доступ к ЭБС «Университетская библиотека онлайн» между БашГУ и «Нексмедиа» № 223-950 от 05.09.2022
4	Договор на доступ к ЭБС «Лань» между БашГУ и издательством «Лань» № 223-948 от 05.09.2022
5	Договор на доступ к ЭБС «Лань» между БашГУ и издательством «Лань» № 223-949 от 05.09.2022

6	Соглашение о сотрудничестве между БашГУ и издательством «Лань» № 5 от 05.09.2022
7	ЭБС «ЭБ БашГУ», бессрочный договор между БашГУ и ООО «Открытые библиотечные системы» № 095 от 01.09.2014 г.
8	Договор на БД диссертаций между БашГУ и РГБ № 223-796 от 27.07.2022
9	Договор о подключении к НЭБ и о предоставлении доступа к объектам НЭБ между БашГУ в лице директора СФ БашГУ с ФГБУ «РГБ» № 101/НЭБ/1438-П от 11.06.2019
10	Договор на доступ к ЭБС «ЭБС ЮРАЙТ» (полная коллекция) между УУНиТ в лице директора СФ УУНиТ и ООО «Электронное издательство ЮРАЙТ» № 1/23-эбс от 03.03.2023

Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»)

№ п/п	Адрес (URL)	Описание страницы
1	http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?a_id=cs_teach_kids	Вопросы безопасности — сайт от компании Symantec
2	http://www.microsoft.com/rus/protect/default.msp#	Вопросы обеспечения информационной безопасности от компании Microsoft
3	http://www.oszone.net/6213/	Обеспечение безопасности детей при работе в Интернет (статья, ссылки, материалы)
4	http://www.anti-malware.ru/	Независимый информационно-аналитический портал по безопасности
5	http://www.securitylab.ru/software/1423/	Каталог программ «Защита детей от интернет угроз» (описание, сравнение, оценки)
6	http://download.live.com/familysafety	Семейная

		безопасность — Windows Live - программа от компании Microsoft
7	http://nicekit.ru/	Программа родительского контроля
8	http://www.etika.ru/	Этика — сайт создан специально для пользователей Рунета, которые хотят работать в этичной, корректной и безопасной среде и готовы участвовать в создании такой среды
9	http://ru.wikipedia.org/wiki/Netiquette	Сетевой этикет — Википедия
10	http://www.antispam.ru/	Проект Антиспам.Ру
11	http://laste.arvutikaitse.ee/rus/html/etusivu.htm	Основы безопасности в Интернете для молодежи интерактивны й курс по Интернет- безопасности
12	http://www.content-filtering.ru/	Интернет- СМИ "Ваш личный Интернет" - помощь родителям в организации безопасного доступа детей в сеть Интернет
13	http://www.citforum.ru/security/	CITFORUM — информацион

		ная безопасность (большое количество материалов по теме)
14	https://securelist.ru/enciklopediya	Энциклопедия информацион ной безопасности
15	http://www.itn.ru/communities.aspx?cat_no=71586&tmpl=com	Обеспечение информацион ной безопасности в учебных заведениях. 4 этапа защиты компьютера — советы от компании Microsoft.
16	http://www.infoforum.ru/	Национальны й форум информацион ной безопасности "ИНФОФОРУ М" — электронное периодическо е издание по вопросам информацион ной безопасности
17	http://saferinternet.ru/	Портал Российского Оргкомитета по проведению Года Безопасного Интернета (ресурсы, ссылки, документы, материалы по проблематике)
18	http://www.securityportal.ru/	Сайт по защите информации,

		защите приватности, безопасным сетевым взаимодейств иям, криптографии
19	http://internetsecure.ru/	Набор технологий и программ для безопасной работы в сети с компьютером

6.3. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Наименование программного обеспечения
Windows 10 Education N / Бессрочная / Microsoft Imagine. Подписка №8001361124 от 04.10.2017 г.
Office Standart 2010 RUS OLP NL Acdmc / 200, Бессрочная / ООО «Компания Фермо» / № Ф-04211 от 12.03.2021
Kaspersky Endpoint Security / 950 / ООО «Смартлайн»/ №44/013 от 06.12.2021
Visual Studio Community 2019 v.16.3 / OLP. Бессрочная / https://visualstudio.microsoft.com/ru/vs/community/
AcademicEdition Networked Volume Licenses RAD Studio XE5 Professional Concurrent App / Плавающая – 60 шт. Бессрочная / ООО«Фермомобайл» / № 04182 от 03.12.2013

7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Тип учебной аудитории	Оснащенность учебной аудитории
Лаборатория информатики и вычислительной техники. Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций, учебная аудитория курсового проектирования (выполнения курсовых работ)	Доска, проектор, экран, учебная мебель, компьютеры, учебно-наглядные пособия.
Специально-оборудованный кабинет в области информатики, технологий и методов программирования. Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и	Доска, проектор, экран, учебная мебель, компьютеры, учебно-наглядные пособия.

промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций.	
Лаборатория аппаратных средств вычислительной техники. Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций	Доска, проектор, экран, учебная мебель, компьютеры, учебно-наглядные пособия.
Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций.	Доска, проектор, экран, учебная мебель, компьютеры, учебно-наглядные пособия.
Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций	Доска, учебная мебель, проектор, экран, учебно-наглядные пособия.
Учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий семинарского типа, учебная аудитория текущего контроля и промежуточной аттестации, учебная аудитория групповых и индивидуальных консультаций, учебная аудитория курсового проектирования (выполнения курсовых работ)	Доска, учебная мебель, компьютеры, проектор, экран, учебно-наглядные пособия.
Лаборатория технической защиты информации. Помещение для проведения учебных занятий семинарского типа, групповых и индивидуальных консультаций	Компьютеры; учебно-наглядные пособия; специализированное оборудование по защите информации от утечки по акустическому каналу, каналу побочных электромагнитных излучений и наводок; технические средства контроля эффективности защиты информации от утечки по каналам.
Читальный зал: помещение для самостоятельной работы	учебная мебель, учебно-наглядные пособия, компьютеры