Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования «Северо-Осетинский государственный университет

имени Коста Левановича Хетагурова»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«**Интернет вещей**»

Направление подготовки:

01.03.02 Прикладная математика и информатика

Профиль: «Программирование, анализ данных

и математическое моделирование»

Квалификация (степень) выпускника – бакалавр

Форма обучения – очная

Год начала подготовки 2024

Владикавказ

2024

Рабочая программа

*обсуждена и утверждена* на заседании кафедры физики и астрономии;

*одобрена* советом факультета математики и компьютерных наук (протокол № 6 от 01.03.2024 г.);

*утверждена* в составе Основной профессиональной образовательной программы понаправлению подготовки 01.03.02 «Прикладная математика и информатика», профиль: «Программирование, анализ данных и математическое моделирование», год начала подготовки 2024 (решение ученого совета от 28.03.2024, протокол № 8).

Составитель: старший преподаватель кафедры физики и астрономии Березов А.В.

**1. Структура и общая трудоемкость дисциплины**

Общая трудоемкость дисциплины составляет 2 з.е. (72 ч.).

|  |  |
| --- | --- |
|  | Очная форма обучения |
| Курс | 4 |
| Семестр | 7 |
| Лекции | 18 |
| Практические занятия | - |
| Лабораторные занятия | 18 |
| Консультации |  |
| Итого аудиторных занятий | 36 |
| Самостоятельная работа | 36 |
| Курсовая работа | - |
| Зачет | + |
| Экзамен | - |
| Общее количество часов | 72 ч. |

**2. Цели изучения дисциплины**

Целями освоения дисциплины «Кибербезопасность и интернет-вещей» являются изучение:

* основных направлений деятельности по обеспечению безопасности Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры;
* основных понятий в области безопасности Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры (КИИ);
* основных угроз, уязвимостей, рисков в области безопасности Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры;
* технологий угроз сетевой безопасности, а также механизмов противодействия сетевым атакам;
* основных требований нормативно-правовых документов по защите объектов критической информационной инфраструктуры;
* особенностей проектирования систем безопасности объектов критической информационной инфраструктуры.

**3. Место дисциплины в структуре ОПОП:**

ФТД.03. Факультативная дисциплина.

Для изучения дисциплины необходимы знания, полученные обучающимися в рамках школьного курса «Информатика», а также в результате освоения дисциплин: «Основы аппаратного и программного обеспечения ПК», «Дискретная математика», «Основы сетевых технологий (CISCO)».

Приступая к изучению дисциплины «Кибербезопасность и интернет-вещей», студент должен иметь представление о базовых понятиях в инфокоммуникационных системах и сетях.

**4. Требования к результатам освоения дисциплины**

Компетенции обучающегося, формируемые в результате освоения дисциплины.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями (результатами освоения образовательной программы):

Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (УК-1);

Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2).

Взаимосвязь планируемых результатов обучения по дисциплине с формируемыми компетенциями ОПОП:

|  |  |  |  |
| --- | --- | --- | --- |
| **Код и формулировка компетенции** | **Планируемые результаты обучения, соответствующие формируемым компетенциям ОПОП** | | |
| **Знать:** | **Уметь** | **Владеть:** |
| УК-1  Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач | порядок определения источников информации, порядок получения доступа к ним;  методы описания и формализации полученной информации;  способы верификации получаемой информации;  принципы системного подхода;  стратегию действий на основе системного подхода, используя обработанную полученную информацию. | использовать способы совершенствования деятельности;  умеет использовать способы и приемы самооценки;  использовать способы определения приоритетов деятельности | навыками критического анализа проблемных ситуаций; |
| УК-2  Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений | принципы социальной ответственности;  принципы построения профессиональной деятельности и бизнеса;  угрозы и риски для граждан и общества в области безопасности «Интернета вещей» и критической информационной инфраструктуры, ответственность за нарушения требований безопасности. | формировать требований к кибербезопасности (информационной безопасности) систем «Интернета вещей», объектов КИИ;  выявлять актуальные угрозы кибербезопасности (информационной безопасности) в системах «Интернета вещей» и объектов КИИ, разрабатывать неформализованные модели угроз;  разрабатывать неформализованные модели средств, систем и процессов, применяемых в системах «Интернета вещей» и объектов КИИ, анализировать их с точки зрения кибербезопасности (информационной безопасности) и проверять адекватность фактическим средствам, системам и процессам;  использовать для построения и проверки моделей пакеты программ анализа и синтеза инфокоммуникационных систем, сетей и устройств | навыками составления практических рекомендаций по использованию результатов научных исследований для организации работ по исследованию кибербезопасности (информационной безопасности) «Интернета вещей» и объектов КИИ;  навыками выполнения работ по обеспечению функционирования систем «Интернета вещей», объектов КИИ в части выполнения требований информационной безопасности (кибербезопасности);  навыками управления технологическими изменениями, нахождения путей совершенствования в части модернизации систем кибербезопасности |

**5. Содержание и учебно-методическая карта дисциплины**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Наименование тем (вопросов), изучаемых по данной**  **дисциплине** | Занятия | | **Самостоятельная работа**  **студентов** | | **Формы контроля** | **Литература** |
| л | лаб | Содержание | Часы |
| 1 | Кибербезопасность: основные понятия и определения.  Киберфизические системы и «Интернет-вещей» - соотношение понятий  Кибербезопасность (информационная безопасность) киберфизических систем, кибербезопасность в «Интернет-вещей»: основные стандарты, понятия, определения. Киберфизические системы и «Интернет-вещей»: обзор основных проблем, связанных с кибербезопасностью; основные угрозы и уязвимости в сфере кибербезопасности.  Регулирование вопросов кибербезопасности в «Интернет- вещей»: международное, в РФ. | 2 | 2 | основные требования к специалистам в области кибербезопасности «Интернет-вещей», критической информационной инфраструктуры | 5 | опрос,  конспект | [1-5] |
| 2 | Сетевые технологии и протоколы: основные понятия и определения.  Сетевые технологии и протоколы – модель OSI, проблемы безопасности  Протоколы связи и аутентификации для киберфизических систем и «Интернет-вещей»: обзор, особенности, проблемы безопасности. | 2 | 2 | классификация и примеры продуктов «Интернет-вещей» для граждан, примеров угроз, уязвимостей, рисков | 5 | опрос,  конспект | [1-5] |
| 3 | Функциональная безопасность: основные понятия и определения.  Функциональная безопасность: основные стандарты, понятия и определения.  Обзор основных стандартов в сфере функциональной безопасности. | 2 | 2 | основные риски и проблемы кибербезопасности «Интернет-вещей» в сфере здравоохранения | 5 | опрос,  конспект | [1-5] |
| 4 | Кибербезопасность в «Интернет-вещей».  Кибербезопасность в «Интернет- вещей» для граждан: классификация продуктов «Интернет- вещей» для граждан, угрозы, уязвимости, риски на примере популярных продуктов.  «Интернет-вещей» в сфере здравоохранения – риски и проблемы.  «Умный дом» - риски и проблемы.  Юридические инциденты – примеры  Цели обеспечения кибербезопасности в «Интернет-вещей» для граждан. | 2 | 2 | основные риски и проблемы кибербезопасности для «Умного дома» | 5 | опрос,  конспект | [1-5] |
| 5 | Кибербезопасность для систем «Умного города».  «Умный город»: состав систем (категории систем, классификация), зрелость Smart City: понятие, критерии оценки, угрозы, риски и проблемы, модель угроз (структура, особенности), обзор стандартов по направлению «Умный город» (Smart City).  «Интернет-вещей» и его применение в Smart Grid, проблемы кибербезопасности | 4 | 4 | состав и классификация систем для «Умного города», критериев оценки безопасности, основные угрозы, риски и проблемы, структуры и особенности построения модели угроз | 5 | опрос,  конспект | [1-5] |
| 6 | Кибербезопасность в «Интернет-вещей» в промышленности.  Киберфизические системы и «Интернет-вещей» в промышленности: понятие «Индустриальный Интернет-вещей», соотношение с понятием «киберфизическая система», классификация продуктов «Интернет- вещей», соотношение с понятиями АСУТП, ICS; угрозы, уязвимости, риски. | 2 | 2 | основные риски и проблемы кибербезопасности в Smart Grid | 5 | опрос,  конспект | [1-5] |
| 7 | Критическая информационная инфраструктура: основные понятия, определения, проектирование систем безопасности.  Критическая информационная инфраструктура, основные понятия, стандарты.  Критическая информационная инфраструктура РФ, основные понятия, НПА, требования  Категорирование объектов КИИ РФ, порядок и критерии  Основные подсистемы обеспечения ИБ объектов КИИ.  Средства обеспечения кибербезопасности (обзор)  Проектирование систем безопасности значимых объектов КИИ  Силы обеспечения кибербезопасности объектов КИИ  Требования к специалистам в области кибербезопасности «Интернет-вещей», критической информационной инфраструктуры.  Построение СМИБ для объектов КИИ на промышленных объектах: Обзор стандартов семейства ISO / ГОСТ 27К. Состав СМИБ. Особенности создания СМИБ для объектов КИИ на промышленных объектах  Ответственность за нарушение требований законодательства РФ в сфере обеспечения безопасности КИИ и КВО ТЭК. | 4 | 2 | основные риски и проблемы кибербезопасности в Индустриальном Интернете вещей | 8 | опрос,  конспект | [1-5] |
|  | **ИТОГО** | 18 | 16 |  | 38 |  |  |

**6. Образовательные технологии**

Согласно учебному плану при преподавании дисциплины используются традиционные образовательные технологии: лекции, лабораторные работы и самостоятельная работа студентов. Также при проведении занятий и самостоятельной работе студентов могут быть использованы современные интерактивные и информационно-коммуникационные образовательные технологии такие как:

– видео-лекция – снятая на камеру сокращенная лекция, дополненная фотографиями и схемами, иллюстрирующая подаваемый в лекции материал;

– интерактивная лекция представляет собой выступление преподавателя перед студенческой аудиторий с применением следующих интерактивных форм обучения: управляемая дискуссия или беседа; демонстрация слайдов или учебных фильмов; мотивационная речь и др.;

**–** видеоконференция – это технология интерактивного взаимодействия двух и более участников образовательного процесса для обмена информацией в реальном режиме времени;

**–** онлайн-семинар – разновидность веб-конференции, проведение онлайн-встреч или презентаций через Интернет в режиме реального времени;

**–** творческое задание требует от студента воспроизведения полученной ранее информации в форме, определяемой преподавателем и требующей творческого подхода: подбор материалов по заданной теме; подбор примеров из практики; самостоятельная постановка и решение нетиповых практических задач;

**–** презентация проекта **–** слайд-презентации позволяют эффектно и наглядно представить содержание, выделить и проиллюстрировать сообщение.

**7. Учебно-методическое обеспечение самостоятельной работы**

По дисциплине предусмотрены следующие виды самостоятельной работы студентов:

– самостоятельное повторение и изучение теоретического материала;

– подготовка доклада по теме, вынесенной на самостоятельное изучение (в форме презентации);

– подготовка к выполнению практических работ;

– подготовка к зачету/экзамену.

Содержание, трудоемкость и формы контроля внеаудиторной самостоятельной работы содержатся в разделе 5, табл. 5.1.

Для обеспечения самостоятельной работы студентов предусмотрены следующие методические материалы (см. разделы 8–9): примерные задания для подготовки к рубежным контрольным работам, перечень тем практических работ, перечень вопросов для подготовки к зачету, перечень рекомендованной литературы. При необходимости дополнительные методические материалы для обеспечения самостоятельной работы студентов размещаются на дистанционной площадке СОГУ начале каждого семестра.

**8. Оценочные средства для текущего контроля успеваемости, рубежной аттестации**

**и промежуточной аттестации по итогам освоения дисциплины**

*Основными формами текущего контроля* по дисциплине являются устный доклад по теме, вынесенной на самостоятельное изучение, выполнение лабораторной работы.

*Форма рубежного контроля:* тест/контрольная работа.

*Формы промежуточной аттестации:* зачет.

Студенты, набравшие в ходе текущего и рубежного контроля необходимое количество баллов, автоматически получают «зачет» или экзаменационную оценку, в соответствии с действующей бально-рейтинговой системой.

**8.1. Формы контроля и критерии оценивания**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Этап** | **Форма**  **контроля** | **Критерии оценивания (процент от максимального кол-ва баллов)** | | | |
| **86-100 %** | **71–85%** | **56–70%** | **Менее 56%** |
| **отлично / зачет** | **хорошо / зачет** | **удовлетворительно / зачет** | **неудовлетворительно / незачет** |
| *1. Текущий контроль (max 20 баллов за 1 модуль)* | | | | | |
|  |  | 15–17 баллов | 12–14 баллов | 9–11 баллов | 0–8 баллов |
|  | Текущая работа в течение модуля  (мах 17б.) | Студент активно работает на занятиях, превосходно выполняет все задания преподавателя. | Студент активно работает на занятиях, хорошо выполняет задания преподавателя. | Студент недостаточно активно работает на занятиях, удовлетворительно выполняет задания преподавателя. | Студент недостаточно активно работает на занятиях, неудовлетворительно выполняет задания преподавателя. |
|  |  | 3 балла | 2 балла | 1 балл | 0 баллов |
|  | Реферат,  доклад, опорный конспект  (мах 3б.) | Тема полностью раскрыта. Превосходное владение материалом. Высокий уровень самостоятельности, логичности, аргументированности. Превосходный стиль изложения. | Тема в основном раскрыта. Хорошее владение материалом. Средний уровень самостоятельности, логичности, аргументированности. Хороший стиль изложения. | Тема частично раскрыта. Удовлетворительное владение материалом. Низкий уровень самостоятельности, логичности, аргументированности. Удовлетворительный стиль изложения. | Тема не раскрыта. Неудовлетворительное владение материалом. Недостаточный уровень самостоятельности, логичности, аргументированности. Неудовлетворительный стиль изложения. |
| *2. Рубежный контроль (15 б. за 1 модуль)* | | | | | |
|  | тест/контрольная работа | Количество баллов за выполнение каждого задания указываются в тесте/контрольной работе. | | | |
| *3. Промежуточная аттестация по дисциплине (max число баллов – в соответствии с действующей балльно-рейтинговой системой)* | | | | | |
|  |  | Критерии оценивания (процент от максимального кол-ва баллов) | | | |
|  |  | 86–100 % | 71–85 % | 50–70 % | 0–49 % |
|  | зачет/экзамен | Дан полный, развернутый ответ на поставленный вопрос. Ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента. | Дан полный ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Но допущены незначительные ошибки, исправленные студентом с помощью «наводящих» вопросов преподавателя. | Дан недостаточно полный ответ. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. Речевое оформление требует поправок, коррекции. | Не получены ответы по базовым вопросам дисциплины или дан неполный ответ и допущены грубые ошибки. Речь неграмотная. Уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины. |

Пересчет полученной суммы баллов по дисциплине в оценку производится согласно действующей балльно-рейтинговой системе.

**8.2. Примерный вариант 1 рубежной контрольной работы (теста) (15 баллов)**

1. Состав и классификация систем для «Умного города», критерии оценки безопасности, основных угроз, рисков и проблем, структуры и особенностей построения модели угроз; (10б)
2. Основные требования к специалистам в области кибербезопасности «Интернет-вещей», критической информационной инфраструктуры.(5б)

**8.3. Примерный вариант 2 рубежной контрольной работы (теста) (15 баллов)**

1. Какой из списков решений относится к индустриальному интернету вещей?

* Мониторинг открытия канализационных люков, автоматизированный магазин без кассиров и продавцов, счетчики воды в домах, которые автоматически передают показания в ЕИРЦ.
* «Умная» домашняя колонка от Amazon, Яндекс или Google, автополив домашних растений, фитнес-прибор, который следит за правильной осанкой человека.

2. Какой термин не существовал до появление интернета вещей?

* АСКУЭ
* АСУТП
* Вавиот

3. Вас просят помочь с выбором датчика влажности для теплиц: задача состоит в том, чтобы замерять уровень влаги и в почве, и в воздухе, а при сильном падении или разнице уровней включать систему орошения. Что вы посоветуете?

* Датчик AM2302 DHT22
* Датчик CCS811 HDC1080
* Датчик RS485
* Посоветую подключить к обсуждению инженера: данных мало, выбор датчиков большой

4. Какой из элементов умного замка, который открывается благодаря Bluetooth-команде с телефона, не обязателен?

* Датчик
* Актуатор (Исполнительное устройство)
* Батарея или иной источник питания
* Микроконтроллер
* Радиомодуль

5. Вы уже знаете, что в зависимости от задачи мы можем добавлять и убирать из устройства какие-то компоненты. Но без каких трех элементов точно невозможно представить наше устройство в системе интернета вещей?

* Батарея или иной источник питания, микроконтроллер, радиомодуль.
* Датчик, актуатор (исполнительное устройство), батарея или иной источник питания.
* Актуатор (Исполнительное устройство), батарея или иной источник питания, микроконтроллер.

6. Представьте, что вам нужно подключить готовое устройство, электронный термостат, к интернету вещей, чтобы собирать информацию о температуре воды в трубах, идущих в подвале дома. Что нужно добавить к нему?

* микроконтроллер
* питание
* исполнительное устройство (актуатор)
* wifi-роутер

7. Какой из этих факторов нужно учитывать при выборе датчика в первую очередь?

Энергоэффективность

* Габариты (размеры)
* Точность измерений
* Диапазон измерений
* Все факторы нужно учесть

8. В теплице стоят приборы-гигрометры — они выводят уровень влажности на ЖК-дисплеях, встроенных в их корпуса, а сотрудники раз в час обходят территорию и заносят показания в электронный журнал. Можно ли улучшить эту систему?

* Нет, ведь данные уже собираются и оцифровываются.
* Да, можно улучшить процесс записи данных.

9. Что такое микроконтроллер?

* Переключатель режимов работы и тока в устройстве.
* Небольшой компьютер, который управляет устройством в интернете вещей.
* Прибор, который обеспечивает связь устройства с сервером.

10. Датчики метана отправляют данные о содержании газа в воздухе каждые 5 минут, независимо от того, превышен он или нет. Нужно перепрограммировать систему так, чтобы сигнал поступал только в случае опасности. На каком уровне системы эффективнее изменить программу?

* На уровне микроконтроллера
* На уровне сервера
* На уровне платформы

11. Как лучше защитить всю систему интернета вещей?

Написать и использовать свою систему шифрования данных на всех этапах их передачи.

* Скачать и установить антивирусы на всех устройства, базовые станции и серверы.
* Обратиться к специалистам по кибербезопасности и заказать комплекс услуг у них.

12. Мы оснастили батареи в больнице новыми электронными термостатами. Они отслеживают и передают температуру воздуха возле каждой точки установки — если воздух вокруг достаточно прогрелся, на термостат поступает команда перекрыть батарею до момента, пока температура не опустится ниже нормы. Как злоумышленник может навредить нашей системе, если мы не защитили ее достаточно хорошо?

* Подключиться к термостату и отправлять с него ложные данные о температуре.
* Подключиться к серверу и отправить команду всем термостатам на перекрытие батареи.
* Подключиться к термостату и отдать команду перекрыть конкретную батарею.
* Перехватывать и подделывать сигналы, добавлять в систему ложные термостаты, выводить на платформе неверные данные.
* Злоумышленник может сделать абсолютно все вышеперечисленное.

13. Что из этого — названия платформ интернета вещей? Если вы не уверены, поищите ответ в интернете.

* Amazon Prime, Zigbee
* Bluetooth, DecaWave, Яндекс.Облако
* Microsoft Azure, IBM Bluem

**8.4. Вопросы к зачету**

1. основные понятия в области кибербезопасности Интернета вещей; основные угрозы, риски и уязвимости в сфере кибербезопасности Интернета вещей и критической информационной инфраструктуры;
2. основные протоколы передачи данных и аутентификации, используемые в «Интернет вещей»;
3. основные понятия в сфере функциональной безопасности;
4. положения основных нормативных актов, регулирующих сферу безопасности критической информационной инфраструктуры Российской Федерации;
5. архитектура основных подсистем обеспечения ИБ объектов КИИ;
6. основные определения СМИБ и особенности построения СМИБ для объектов КИИ на промышленных объектах;
7. положения нормативных актов, устанавливающих ответственность за нарушение требований законодательства РФ в сфере обеспечения безопасности КИИ и КВО ТЭК.
8. основные средства обеспечения кибербезопасности (архитектура, принципы построения);
9. принципы проектирования систем безопасности значимых объектов КИИ;
10. состав и способы организации деятельности сил обеспечения кибербезопасности объектов КИИ;
11. основные требования к специалистам в области кибербезопасности «Интернет-вещей», критической информационной инфраструктуры;
12. цели обеспечения кибербезопасности в «Интернет-вещей» для граждан;
13. классификация и примеры продуктов «Интернет-вещей» для граждан, примеры угроз, уязвимостей, рисков;
14. основные риски и проблемы кибербезопасности «Интернет-вещей» в сфере здравоохранения;
15. основные риски и проблемы кибербезопасности для «Умного дома»;
16. состав и классификация систем для «Умного города», критерии оценки безопасности, основных угроз, рисков и проблем, структуры и особенностей построения модели угроз;
17. основные риски и проблемы кибербезопасности в Smart Grid;
18. основные риски и проблемы кибербезопасности в Индустриальном Интернете вещей;
19. примеры юридических инцидентов в области регулирования кибербезопасности «Интернета-вещей».

**9. Учебно-методическое и информационное обеспечение дисциплины**

**а) основная литература:**

1. Дубков, И.С. Решение практических задач на базе технологии интернета вещей : учебное пособие : [16+] / И.С. Дубков, П.С. Сташевский, И.Н. Яковина ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2017. – 80 с. : ил.,табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=576635> – Библиогр. в кн. – ISBN 978-5-7782-3161-0. – Текст : электронный.
2. Изотов, И.Н. Разработка системы интернета вещей «Свежий воздух»: выпускная квалификационная работа / И.Н. Изотов ; Уральский федеральный университет им. первого Президента России Б. Н. Ельцина, Институт радиоэлектроники и информационных технологий – РтФ, Школа бакалавриата. – Екатеринбург : б.и., 2019. – 66 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=563483> – Текст : электронный.
3. Колесников, М.В. Исследование и разработка интеллектуальных контроллеров для промышленного интернета вещей: выпускная квалификационная работа / М.В. Колесников ; Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Факультет СуиР. – Санкт-Петербург : б.и., 2019. – 62 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=562997> – Текст : электронный.

**б) дополнительная литература:**

1. Беспроводные технологии / гл. ред. П. Правосудов ; учред. ООО «Издательство Файнстрит», Г.А. Дружинина. – Санкт-Петербург : Медиа КиТ, 2015. – № 4(41). – 68 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=430233>. – ISSN 2079-9233. – Текст : электронный.
2. Филимонова, А.А. Разработка ПО, обеспечивающего безопасность помещения с помощью «умных вещей» / А.А. Филимонова ; Амурский государственный университет (АмГУ). – Благовещенск  : б.и., 2020. – 66 с. : ил., табл., схем – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=596766> – Текст : электронный.

***в) Профессиональные базы данных и другие интернет-ресурсы:***

– ЭБС «Научная электронная библиотека eLibrary.ru» (<http://www.elibrary.ru>);

– ЭБС «Университетская библиотека online» (<http://www.biblioclub.ru>);

– ЭБС «Юрайт» (<http://biblio-online.ru>);

– ЭБС «Консультант студента» ([studentlibrary.ru](https://www.studentlibrary.ru/)).

**10. Материально-техническое обеспечение дисциплины**

Для проведения лекционных и лабораторных занятий используются:

– учебные аудитории для проведения лекционных занятий, занятий семинарского типа, текущего контроля, промежуточной аттестации, оборудованные аудиторной мебелью, доской (меловой, маркерной или интерактивной), компьютером или ноутбуком с возможностью подключения к сети «Интернет» и доступом в электронную информационно-образовательную среду СОГУ, мультимедийным проектором, экраном;

– компьютерный класс (корпус 10, ауд. 605, 606), оборудованный аудиторной мебелью, доской (меловой, маркерной или интерактивной), компьютерами или ноутбуками с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде СОГУ, мультимедийным проектором, экраном.

*Лицензионное программное обеспечение:*

1. Windows 10 Pro for Workstations, (№ 4100072800 Microsoft Products (MPSA) от 04.2016г);
2. Office Standard 2016 (№ 4100072800 Microsoft Products (MPSA) от 04.2016г);
3. Система поиска текстовых заимствований «Антиплагиат ВУЗ»;

*Перечень ПО в свободном доступе:* Kaspersky Free; WinRar; Google Chrome; Yandex Browser; Opera Browser; Acrobat Reader;

Помещение для самостоятельной работы студентов: Зал электронных ресурсов Научной библиотеки СОГУ (корпус 6, кабинет № 1.8), укомплектован специализированной мебелью (рабочие места студентов), необходимыми техническими средствами обучения: компьютеры, принтер, возможность подключения к сети «Интернет», доступ в электронную информационно-образовательную среду СОГУ.