

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

УТВЕРЖДАЮ

Декан факультета Трещев И.А.

ФИО декана

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Интернет вещей»

Направление подготовки	<i>09.04.01 Информатика и вычислительная техника</i>
Направленность (профиль) образовательной программы	<i>«Информационное и программное обеспечение вычислительной техники и автоматизированных систем»</i>

Обеспечивающее подразделение
<i>Кафедра ПУРИС – Проектирование, управление и разработка информационных систем</i>

Разработчик рабочей программы:

Декан ФКТ, к.т.н.
(должность, степень, ученое звание)

(подпись)

Трещев И.А.
(ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой
ПУРИС
(наименование кафедры)

(подпись)

А.Н. Петрова

(ФИО)

1 Общие положения

Рабочая программа дисциплины «Алгоритмические языки» составлена в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Министерства образования и науки Российской Федерации №918, и основной профессиональной образовательной программы подготовки «Информационное и программное обеспечение вычислительной техники и автоматизированных систем» по направлению 09.04.01 "Информатика и вычислительная техника".

Задачи дисциплины	Получение представления о системах передачи информации, задачах которые решаются в ходе проектирования, строительства, эксплуатации и оптимизации мультисервисных сетей, систем передачи информации
Основные разделы / темы дисциплины	Раздел 1 Основы : IoT введение, Сеть и интернет вещей Раздел 2 Организация и технология построения сетей связи. Симуляторы сетевого оборудования: Iot. Протоколы, механизмы, взаимодействие, Iot и маршрутизация Промежуточная аттестация: Экзамен

2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины ««Интернет вещей»» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой:

Код и наименование компетенции	Индикаторы достижения	Планируемые результаты обучения по дисциплине
Универсальные		

Общепрофессиональные		
ОПК-1 Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте	ОПК-1.1 Знает математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности ОПК-1.2 Умеет решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных, социально-экономических и	Знает современное программное и аппаратное обеспечение информационных и автоматизированных систем Умеет модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач Владеет современными методами и инструментальными средствами прикладной информатики для автоматизации и информатизации решения прикладных задач

	профессиональных знаний ОПК-1.3 Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте	
--	---	--

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Интернет вещей» изучается на 1 курсе, 2 семестре.

Дисциплина входит в состав блока 1 «Дисциплины (модули)» и относится к базовой части.

Для освоения дисциплины необходимы знания, умения, навыки и / или опыт практической деятельности, сформированные в процессе изучения дисциплин / практик: «Методы оптимизации», «Вычислительная геометрия».

Знания, умения и навыки, сформированные при изучении дисциплины «Интернет вещей», будут востребованы при изучении последующих дисциплин: «Машинное обучение», «Учебная (ознакомительная) практика».

Место дисциплины (этап формирования компетенции) отражено в схеме формирования компетенций, представленной в документе *Оценочные материалы*, размещенном на сайте университета www.knastu.ru / *Наш университет* / *Образование* / *09.04.01 Информатика и вычислительная техника/ Оценочные материалы*).

Дисциплина «Интернет вещей» частично реализуется в форме практической подготовки. Практическая подготовка организуется путем выполнения лабораторных работ, иных видов учебной деятельности.

Дисциплина «Интернет вещей» в рамках воспитательной работы направлена на воспитание чувства ответственности; формирование умения аргументировать, самостоятельно мыслить; развитие творчества, профессиональных умений; формирование системы осознанных знаний, ответственности за выполнение учебно-производственных заданий.

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

4.1 Структура и содержание дисциплины для очной формы обучения

Дисциплина «Интернет вещей» изучается на 1 курсе во 2 семестре.

Общая трудоёмкость дисциплины составляет 4 з.е., 144 ч., в том числе контактная работа обучающихся с преподавателем 48 ч., промежуточная аттестация в форме экзамена

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)					
	Контактная работа преподавателя с обучающимися			ИКР	Пром. аттест.	СРС
	Лекции	Практические занятия	Лабораторные работы			
Раздел 1 Основы функционирования IoT						
IoT введение <i>Эталонная модель OSI и отображение на IoT. Трафик в сетях. Встраиваемые системы и IoT. Поисковые системы интернета вещей. Безопасность IoT. Мониторинг. Операционные системы реального времени и их применение для инфраструктур. Классификация и особенности архитектур операционных систем для IoT. Аппаратные ресурсы. IoT на базе WiFi. Доверенные взаимодействия. Основы построения гетерогенных сетей интернета вещей. Взаимодействие оконечных устройств и "базовых станций", вопросы обеспечения информационной безопасности;</i>	8					

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)					
	Контактная работа преподавателя с обучающимися			ИКР	Пром. аттест.	СРС
	Лекции	Практические занятия	Лабораторные работы			
Сеть и интернет вещей <i>Протоколы интернета вещей, анализ трафика, исследование доверенных взаимодействий, операционные системы реального времени (MbedOs, QNX).</i>			16*			
Расчетно-графическая работа часть 1 <i>Поисковые системы интернет вещей.</i>						30
Раздел 2 Организация и технология построения сетей связи для IoT.						
IoT. Протоколы, механизмы, взаимодействие. <i>Обзор и механизм работы Wi-Fi. Обзор и механизм работы классического Wi-Max. Обзор решений Lora. Структура и место традиционных технологий. Требования к качеству сети. Механизмы обеспечения качества обслуживания &ndash; CoS и QoS. Приоритезация трафика, взвешенная справедливая очередь Структура и механизм работы мобильных сетей 1G, 2G, 3G, 4G. Обзор разработок 5G. Обзор IPv6, взаимодействие с Ethernet. Обзор стека TCP/IPv6. Взаимодействие с IPv4, отличия от IPv4. Маршрутизация RIP;</i>	8*					
IoT и маршрутизация <i>Надежность, доступность, конвергентность, масштабируемость, управляемость и безопасность сети. Обзор механизма работы и социального значения сервисов: Torrent, Skype, поисковик на примере Google, Wikipedia, социальные сети, Shodan. Перспективы развития opensource и проприетарного подхода. Обсуждение легитимности и технической стороны методов сбора пользо-</i>			16*			

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)					
	Контактная работа преподавателя с обучающимися			ИКР	Пром. аттест.	СРС
	Лекции	Практические занятия	Лабораторные работы			
<i>вательских данных. Симуляторы сетей Поиск неисправностей в сети. Сети мобильных абонентов, LoraWAN сети. Устранение неисправностей в сети IoT и перспективы гетерогенных сетей. ZigBee сети. BLE сети.</i>						
Расчетно-графическая работа часть 2 <i>Анализ трафика BLE</i>						30
Экзамен	-	-	-	1	35	36
ИТОГО по дисциплине	16 в том числе в форме практической подготовки: 2	-	32 в том числе в форме практической подготовки: 10	1	35	60

* реализуется в форме практической подготовки

5 Оценочные средства для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонды оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обсуждаются и утверждаются на заседании кафедры. Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов обучения по дисциплине (модулю) хранится на кафедре-разработчике в бумажном или электронном виде, также фонды оценочных средств доступны студентам в личном кабинете – раздел учебно-методическое обеспечение.

6 Учебно-методическое и информационное обеспечение дисциплины (модуля)

6.1 Основная и дополнительная литература

Перечень рекомендуемой основной и дополнительной литературы представлен на сайте университета www.knastu.ru / Наш университет / Образование / 09.04.01 Информатика и вычислительная техника / Рабочий учебный план / Реестр литературы.

6.2 Методические указания для студентов по освоению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.
2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.
3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.
4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

При самостоятельной проработке курса обучающиеся должны:

- просматривать основные определения и факты;
- повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;
- изучить рекомендованную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;
- самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;
- использовать для самопроверки материалы фонда оценочных средств.

6.3 Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Каждому обучающемуся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, с которыми у университета заключен договор.

Перечень рекомендуемых профессиональных баз данных и информационных справочных систем представлен на сайте университета *www.knastu.ru / Наш университет / Образование / 09.04.01 Информатика и вычислительная техника/ Рабочий учебный план / Реестр ЭБС.*

Актуальная информация по заключенным на текущий учебный год договорам приведена на странице Научно-технической библиотеки (НТБ) на сайте университета

<https://knastu.ru/page/3244>

6.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

На странице НТБ можно воспользоваться интернет-ресурсами открытого доступа по укрупненной группе направлений и специальностей (УГНС) 09.00.00 информатика и вычислительная техника. Научная электронная библиотека Elibrary **<http://elibrary.ru>**.

7 Организационно-педагогические условия

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) - русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет соответствующих дисциплин и профессиональных моду-

лей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

7.1 Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно-телекоммуникационной сети «Интернет» по адресу <https://student.knastu.ru>. Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий. Для освоения дисциплины студентам предоставляется доступ на портал ДО ФГБОУ ВО КнАГУ к курсу Телекоммуникационные системы. Часть 2 IoT.

7.2 Занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

7.3 Самостоятельная работа обучающихся по дисциплине (модулю)

Самостоятельная работа студентов – это процесс активного, целенаправленного приобретения студентом новых знаний, умений без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности обучающегося.

Цели самостоятельной работы:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную и справочную документацию, специальную литературу;
- развитие познавательных способностей, активности студентов, ответственности и организованности;
- формирование самостоятельности мышления, творческой инициативы, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений и академических навыков.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, уровня сложности, конкретной тематики.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов университета.

Контроль результатов внеаудиторной самостоятельной работы студентов может проходить в письменной, устной или смешанной форме.

Студенты должны подходить к самостоятельной работе как к наиважнейшему средству закрепления и развития теоретических знаний, выработке единства взглядов на отдельные вопросы курса, приобретения определенных навыков и использования профессиональной литературы.

7.4 Методические рекомендации для обучающихся по освоению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.
2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.
3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.
4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

При самостоятельной проработке курса обучающиеся должны:

- просматривать основные определения и факты;
- повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;
- изучить рекомендованную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;
- самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;
- использовать для самопроверки материалы фонда оценочных средств.

Расчетно-графическая работа часть 1 “Поисковые системы для Интернета Вещей”

1 Цель работы

Целью работы является получение навыков работы с поисковыми системами “Интернета вещей” Shodan и Censys.

2 Краткие теоретические сведения

Современную жизнь нельзя представить без устройств Интернета вещей они окружают людей повсеместно и затрагивают самые разные аспекты жизни. Люди разрешают этим устройствам следить за собой, в надежде что это упростит им жизнь, но при этом забывают, что поскольку все эти устройства подключены к Интернету, к устройствам можно получить оттуда доступ. Для этих целей по аналогии с Google и Яндекс существуют специальные поисковые системы, которые позволяют найти эти подключенные устройства, например, Shodan и Censys.

Принцип работы такой поисковой системы можно представить в виде человека, который ходит по улице и стучится в каждую дверь. В реальности роли дверей выступают адреса устройств, а улица это сеть их объединяющая.

Если это воображаемого человека спросить о дверях, которые есть в конкретном доме, он может, например, рассказать: какие там двери, сколько их, кто ответит на стук и

что эти люди ответят. Применительно к Shodan и Censys это информация об объектах Интернета вещей: как они называются, к какому типу устройств принадлежат и есть ли у них веб-интерфейс, который можно использовать. И если раньше основную долю результатов поиска составляли маршрутизаторы, сетевые принтеры и IP-камеры, то теперь даже некоторые лампочки имеют собственный IP-адрес. Не задумываясь о последствиях к интернету подключают все подряд — от умной бытовой техники до автоматизированных систем управления технологическими процессами.

Использование Shodan

Shodan, по своим потенциальным возможностям, — опасная технология в руках киберпреступников. Но при этом один из самых эффективных инструментов в арсенале у специалистов по сетевой безопасности.

В основе Shodan лежит поисковый робот, подобный «паукам» Google. Он накапливает сведения об узлах сети, ответивших хотя бы на один запрос, в их числе могут быть IP-камеры, умные дома и прочее. Отличие Shodan от Google и других подобных поисковых систем, в том что последние в основном работают с WWW, а Shodan сканирует всё что подключено к Интернету. Его глобальная цель составить карту всего Интернета. Еще одним отличием является то, что Shodan требует жесткого соблюдения синтаксиса запросов, нельзя написать “электростанция” и получить список всех электростанций, имеющих выход в Интернет.

Один из возможных вариантов применения - поиск роутеров с дефолтными паролями, для этого достаточно вбить в поиск “admin admin”. Но это, пожалуй, самое безвредное, что там можно обнаружить. Например, вполне реально обнаружить незащищенные рентгеновские аппараты и посмотреть снимки пациентов или подключиться к оборудованию атомной электростанции.

Но не все так плохо, от использования Shodan есть и польза, он может помочь вам найти уязвимые устройства в ваших собственных сетях, и защитить их, прежде чем кто-то решит воспользоваться этими уязвимостями.

Shodan использует собственный встроенный сканер портов. Основную информацию для анализа Shodan получает из баннеров, с помощью которых сервисы, запущенные на открытых портах, сообщают о себе. Эти баннеры публично объявляют всему Интернету, какие сервисы они представляют и как с ними взаимодействовать. Это может быть информация о программном обеспечении сервера, о том, какие параметры поддерживает сервис, приветственное сообщение или что-то еще, что клиент хотел бы знать, прежде чем начать взаимодействовать с сервером. Вот так выглядит FTP-баннер, в качестве примера приведенный на сайте Shodan:

220 kcg.cz FTP server (Version 6.00LS) ready.

Эта информация позволяет узнать потенциальное имя сервера: kcg.cz, тип: FTP-сервер и его версия: 6.00LS.

Аналогичный пример баннера для HTTP-сервера выглядит так:

HTTP/1.0 200 OK

Date: Tue, 16 Feb 2010 10:03:04 GMT

*Server: Apache/1.3.26 (Unix) AuthMySQL/2.20 PHP/4.1.2 mod_gzip/1.3.19.1a
mod_ssl/2.8.9*

OpenSSL/0.9.6g

Last-Modified: Wed, 01 Jul 1998 08:51:04 GMT

ETag: "135074-61-3599f878"

Accept-Ranges: bytes

Content-Length: 97

Content-Type: text/html

Другие сервисы на других портах также предоставляют специфическую для конкретного сервиса информацию. Естественно, никто не гарантирует, что опубликованный баннер является верным или подлинным, в Shodan можно найти и honeypot (ресурс, представляющий собой приманку для злоумышленников). Но, все же, в большинстве случаев эта информация соответствует истине. Отдельно стоит отметить, что ситуация с использованием этого поисковика классическая для исследователей в области информационной безопасности — инструмент может использоваться как с благими намерениями, так и с целью нарушения закона. В данной работе поисковики будут использоваться только в исследовательских целях.

Существует множество вариантов для применения поисковика Shodan в самых разных областях. Вот некоторые из них:

- сетевая безопасность: следите за всеми устройствами в вашей компании с доступом в Интернет;
- кибер-риски: проводите онлайн-исследования ваших поставщиков с точки зрения оценки рисков;
- маркетинговые исследования: отслеживайте, какие продукты и для каких задач предпочитают использовать потребители по всему миру;
- профилактика заражений: оценивайте, сколько используемых устройств уязвимы к заражению различными вирусами и программами-вымогателями.

Применение Shodan позволяет взглянуть на свою сеть глазами киберпреступников, выявить слабые места и уязвимые устройства. Однако, все же, полностью доверять всей информации, которую он вам демонстрирует, не стоит. Этот поисковый движок в основном работает с баннерами, а баннеры можно изменить, подделать и подменить.

Знакомство с Shodan начинается с регистрации. Попробовать возможности поисковика можно и не регистрируясь, но самые интересные функции открываются после регистрации. Кроме бесплатной существует и несколько вариантов платной регистрации. Бесплатный аккаунт имеет несколько ограничений, например, по количеству результатов и доступным фильтрам (50 в сутки). Доступ к расширенным фильтрам требует платного членства (49\$). Для разработчиков и корпоративных пользователей существуют предложения с ежемесячной платой (с более детальной информацией можно ознакомиться здесь: <https://account.shodan.io/billing>)

Чтобы создать учетную нажмите на кнопку Register, заполните все необходимые поля и затем нажмите на кнопку «Create» (рисунок 1).

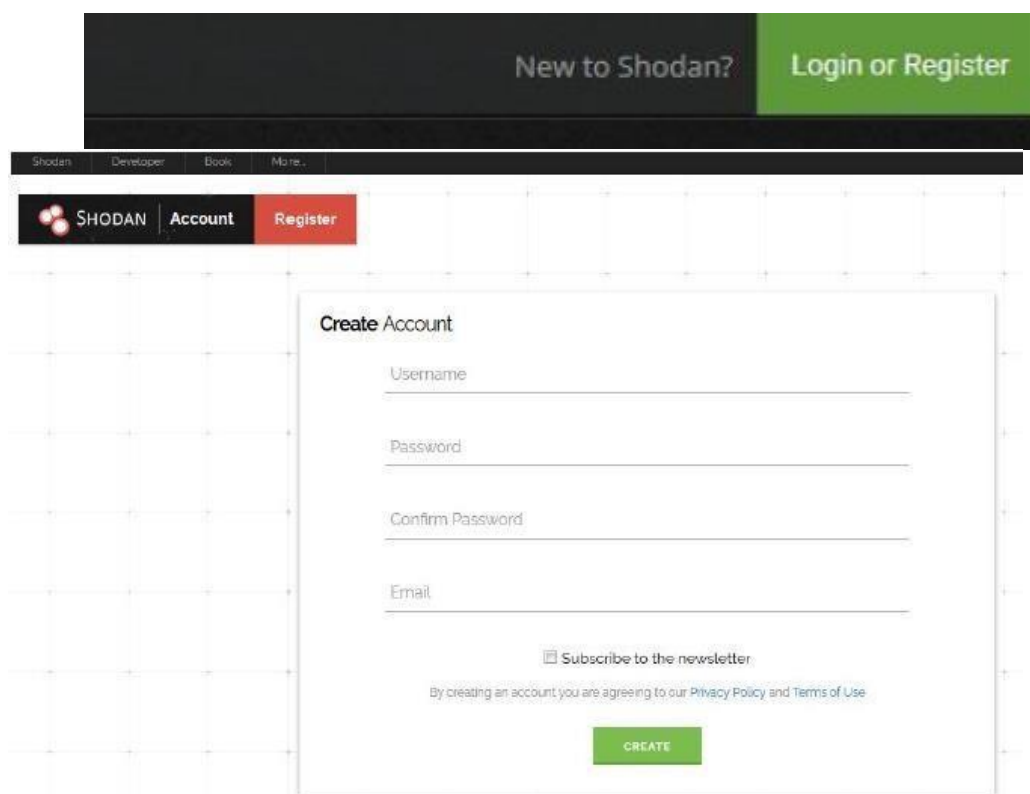


Рисунок 1. Как пользоваться Shodan: Регистрация

Авторизовавшись в системе, начните ознакомление с верхнего меню.

Здесь строка поиска и несколько кнопок (Рисунок 2)



Рисунок 2. Панель меню Shodan

Кнопка «Explore» дает возможность просматривать последние и самые популярные поисковые запросы добавленные пользователями в закладки. Страница разделена на четыре поля.

- Categories - поиск по категориям;
- Top Voted - самые популярные поисковые запросы за все время; □ Filtres - поиск по популярным фильтрам;
- Recently Shared - последние поисковые запросы.

Ниже скрин с подробным описанием каждого элемента страницы:

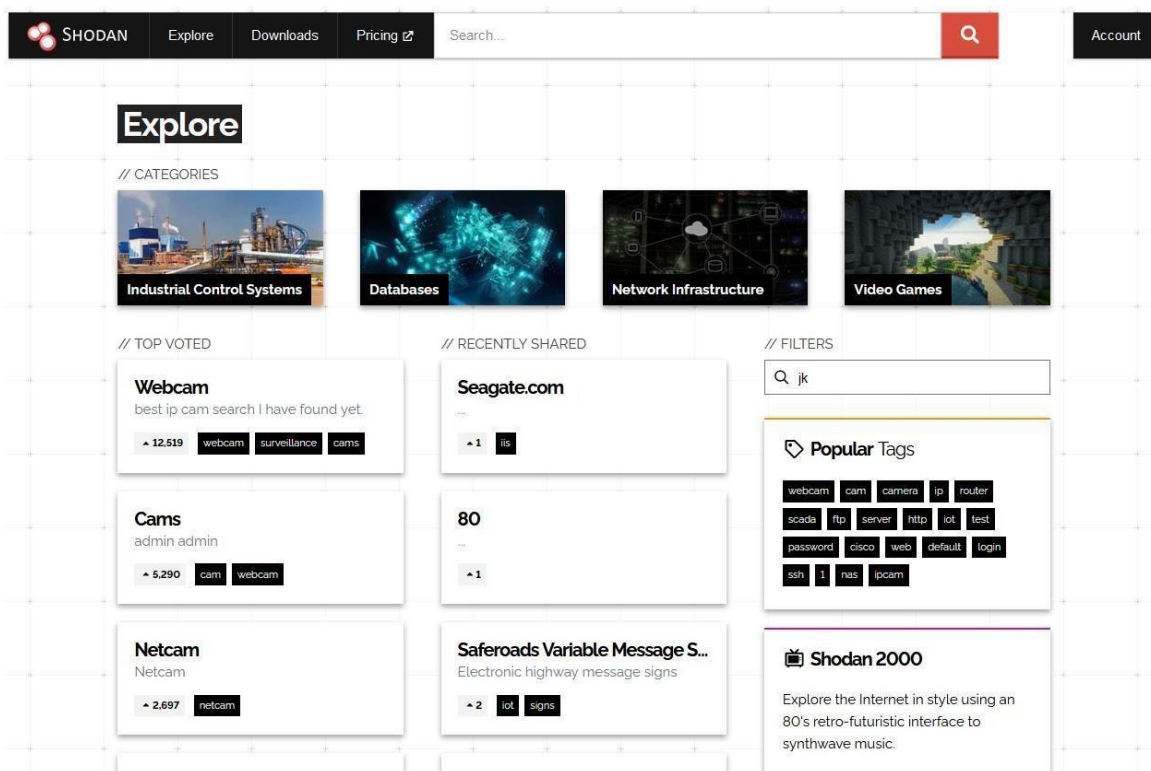


Рисунок 3. Описание элементов Shodan

Нажмите, например, на запрос, «default password». Прочитав описание можно понять, что речь идет о роутерах с паролем по умолчанию.

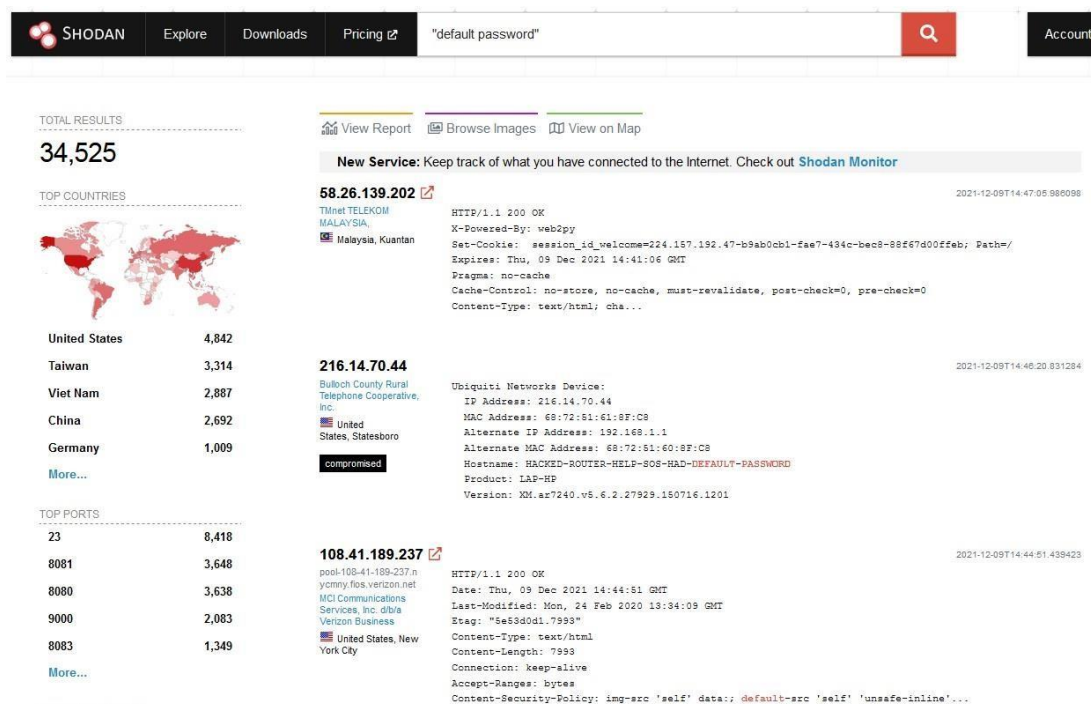


Рисунок 4. Результаты поиска по запросу «default password»

Моментально появляются результаты сканирования. В открывшемся окне слева на право (рисунок 4):

1. в левой части экрана общая информация. Общее число результатов. Результаты по странам и отдельное количество найденных результатов в каждой стране. Провайдеры, порты, операционные системы и т.д;

2. в середине располагаются сами результаты с поверхностной информацией: IP-адрес, провайдер, дата добавления, страна, город. Более подробную информацию можно получить нажав на IP-адрес; 3. поле справа, отображает баннер ответа.

По умолчанию функция поиска сайта использует введенное слово для поиска, как точное выражение для поискового запроса. Поисковик может искать только конечное слово из запроса (к примеру, поисковой запрос «WVC80» вернет только «WVC80» и проигнорирует «WVC80N»), и рассматривает несколько слов только как логическое выражение AND («и»). Общие слова (a, and, by, the, is, on, it) будут игнорироваться.

Основной поиск будет выполнять сопоставление строки с информацией из баннеров серверов без поиска с помощью дополнительных метаданных протокола, которые также собираются из обнаруженных устройств.

В Shodan можно искать устройства определенного производителя. Например, можно поискать устройства Mikrotik с web-интерфейсом доступ к которым возможен без авторизации. Для этого необходимо вспомнить основные коды HTTP-ответов:

- 200 OK Request succeeded;
- 301 Moved Permanently Assigned a new permanentURI;
- 302 Found Resides under a different URI;
- 401 Unauthorized Request requires authentication;
- 403 Forbidden Request is denied regardless of authentication.

Таким образом набрав поисковый запрос вида “200 mikrotik” Shodan выдаст порядка 1 400 000 результатов с устройствами Mikrotik.

Чтобы получить максимум от Shodan важно понимать синтаксис поискового запроса. Как было сказано ранее система работает с баннерами, которые представляют собой информацию о службах запущенных на устройствах. Например, баннер вида:

```
{
  "data": "Moxa Nport Device
    Status: Authentication disabled
    Name: NP5232I_4728
    MAC: 00:90:e8:47:10:2d",
  "ip_str": "46.252.132.235",
  "port": 4800,
  "org": "SingTel Mobile",
  "location": {
    "country_code": "SG"
  }
}
```

Данный баннер имеет 5 свойств, у реальных баннеров количество свойств может быть другим. Каждое свойство хранит различную информацию о запущенных службах:

- data: основной ответ от самого сервиса;
- ip_str: IP-адрес устройства;
- port: номер порта службы;
- org: организация, которая владеет этим диапазоном IP-адресов; □
- location.country_code: страна, в которой находится устройство.

По умолчанию, Shodan ищет только по содержимому свойства data, и оно может существенно различаться в зависимости от типа службы. Поэтому при поиске необходимо определиться, какие именно службы Вас интересуют.

Чтобы поиск осуществлялся не только по свойству “data”, необходимо использовать поисковые фильтры, с их помощью можно сообщить Shodan, что вы хотите выполнить поиск по определенным свойствам. Фильтры имеют формат: **“filtername:value”**.

Обратите внимание, что между именем фильтра и его значением нет пробела.

Чтобы найти устройства, например, в определенной стране, необходимо применить фильтр “country”, и подставить код страны, длиной в два символа.

country:ru

Если значение, которое вы пытаетесь найти, содержит пробелы, необходимо заключить значение в кавычки. Например, следующий поисковый запрос показывает устройства, которые находятся в сети OJSC Sibirtelecom: **org:"OJSC Sibirtelecom"**

Фильтры Shodan также можно комбинировать, чтобы еще больше уточнить результаты. Например, вот поисковый запрос для поиска устройств, расположенных в сети Сибирьтелеком и находящихся в России: **country:"RU" org:"OJSC Sibirtelecom"**

Для понимания работы фильтров и собственно того какие фильтры поддерживаются, можно изучить запросы из числа рейтинговых, а также переходя по ссылкам, уточняющим характеристики запроса. Для примера, можно со страницы **“Explore”** перейти в категорию **“Industrial Control Systems”** и выбрать одну из фирм производителей ПЛК. Каждый производитель из списка характеризуется некоторым набором признаков, позволяющим идентифицировать его оборудование. Например, для ПЛК фирмы Omron характерно использование протокола FINS, данные устройства могут быть обнаружены Shodan с помощью фильтра: **port:9600 response code**

В дальнейшем в окне результатов поиска вы можете задать дальнейшее уточнение по нескольким ключевым областям. На боковой панели слева можно наблюдать некоторые сводные выборки полученных данных:

- карта результатов;
- ТОП-список сервисов (порты);
- ТОП-список организаций (ISP, internet service provider — поставщики интернет-услуги);
- ТОП-список операционных систем;
- ТОП-список продуктов (по названию программного обеспечения).

В основном разделе можно получить расширенный вывод результатов, куда будет включена следующая информация:

- IP-адрес; ☐ имя хоста;
- поставщик интернет-услуг;
- время, когда запись была добавлена в базу данных; ☐ страна, в которой находится устройство; ☐ сам баннер.

Для получения дополнительной информации вы можете кликнуть на **“details”**, которая перенаправит вас непосредственно к информации об этом хосте (рисунок 5).

🌐 128.211.197.206

dhcp-197-206.resnet.purdue.edu

City	Kokomo
Country	United States
Organization	Purdue University
ISP	Purdue University
Operating System	Windows 6.1
Last Update	2020-07-28T07:40:31.717803
Hostnames	dhcp-197-206.resnet.purdue.edu
ASN	AS17

🚪 Ports

22	53	80	137	445
----	----	----	-----	-----

🚪 Services

22
tcp
ssh

OpenSSH Version: 7.6p1 Ubuntu-4ubuntu0.3

```
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAQCN8xfI0HMs
nt4fwNECRtcTQofXW8ggD+wEf2r5XPmzjZe
ta5E018njRq1jXZ1Qmr+55KnVi1PawDBQFwNnPCwbyZ5q
P8bzTH0yIzNsh3bIfx4XN+nTtkUn0H
Zau5lLeJUJ0brbFGx41hMkA1x/NC18cb/p3PECTBT5bmhn
eEZnb1qF60BsqwxMmMdtQavSfsV/j+
RQkE/Tvgi0+tDfDJD0FRuKqIYyP3ACSP3z6h9SpqzYaIUT
eW1JuoojdS1LGmpWZX81wHmUUvSVUQ
HD8F4p1Y8gr71jxxk0V6S5p1NiBEkYS4z0Gj0VJkNGWh6R5
X+MMGKF2Z1uLCWPWjbAR19
Fingerprint: e8:d0:09:38:28:97:4b:a5:44:06:01:
82:6a:cf:0c:04
```

Рисунок 5. Детализация результата запроса

Для улучшения качества поиска, с целью включения/исключения каких-то значений свойств, можно использовать фильтр хэшей свойств: **filter:hash**. Каждый баннер содержит свойство **hash**, которое является числовым хешем свойства **data**. Это может быть полезно, например, чтобы исключить пустые результаты поиска, пустые баннеры всегда имеют одно и то же значение хэша, равное нулю, исключить их из поиска можно добавив **hash:0** к поисковому запросу.

Помимо функции обнаружения устройств и служб Shodan может связывать информацию об устройстве с характерными уязвимостями. С баннерами могут быть связаны уязвимости двух типов: подтвержденные и неподтвержденные. Неподтвержденные уязвимости - это уязвимости, которые подразумеваются на основе собранных метаданных. Например, если на сервере работает старая версия Apache, то Shodan свяжет известные проблемы с этой версией и установит для связанного свойства **“verified”** в баннере значение False, если обнаружена подтвержденная уязвимость, то будет установлено значение True. Неподтвержденные уязвимости могут представлять собой ложные срабатывания в зависимости от устройства/программного обеспечения, поэтому они обычно требуют дополнительной проверки, чтобы убедиться, что служба уязвима. Их следует рассматривать как отправную точку для дальнейшего расследования (рисунок 6).

⚠️ Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2010-2068	mod_proxy_http.c in mod_proxy_http in the Apache HTTP Server 2.2.9 through 2.2.15, 2.3.4-alpha, and 2.3.5-alpha on Windows, NetWare, and OS/2, in certain configurations
---------------	--

Рисунок 6. Пример отображения уязвимости.

Вся информация об уязвимостях хранится в свойстве “**vulns**” в баннере. Вы можете увидеть, как это выглядит, на вкладке “**Raw**” на странице информации или непосредственно взглянув на ответ API. Свойство “**vulns**” - это объект, ключи которого представляют собой идентификаторы уязвимости (например, CVE-2014-0160), а значения содержат информацию об уязвимости. Подробнее ознакомиться со свойствами и фильтрами на их основе можно на <https://datapedia.shodan.io/>

Помимо поиска и просмотра свойств баннеров Shodan позволяет выгрузить информацию для анализа информации внешними автоматизированными инструментами. Возможна выгрузка в json, csv, xml. Но стоит отметить что возможности выгрузке на бесплатном аккаунте не доступны.

Использование Censys

Долгое время Shodan был единственным поисковым движком по Интернету вещей. В 2013 году возник Censys — его бесплатный конкурент. Он подобно Shodan, опрашивает все публично доступные IP-адреса и протоколирует их отклики., вот только создатели Censys дополнительно сделали упор на поиск уязвимостей. Censys может выдать список устройств, не защищенных от какой-то конкретной известной угрозы из числа наиболее распространенных (рисунок 7).

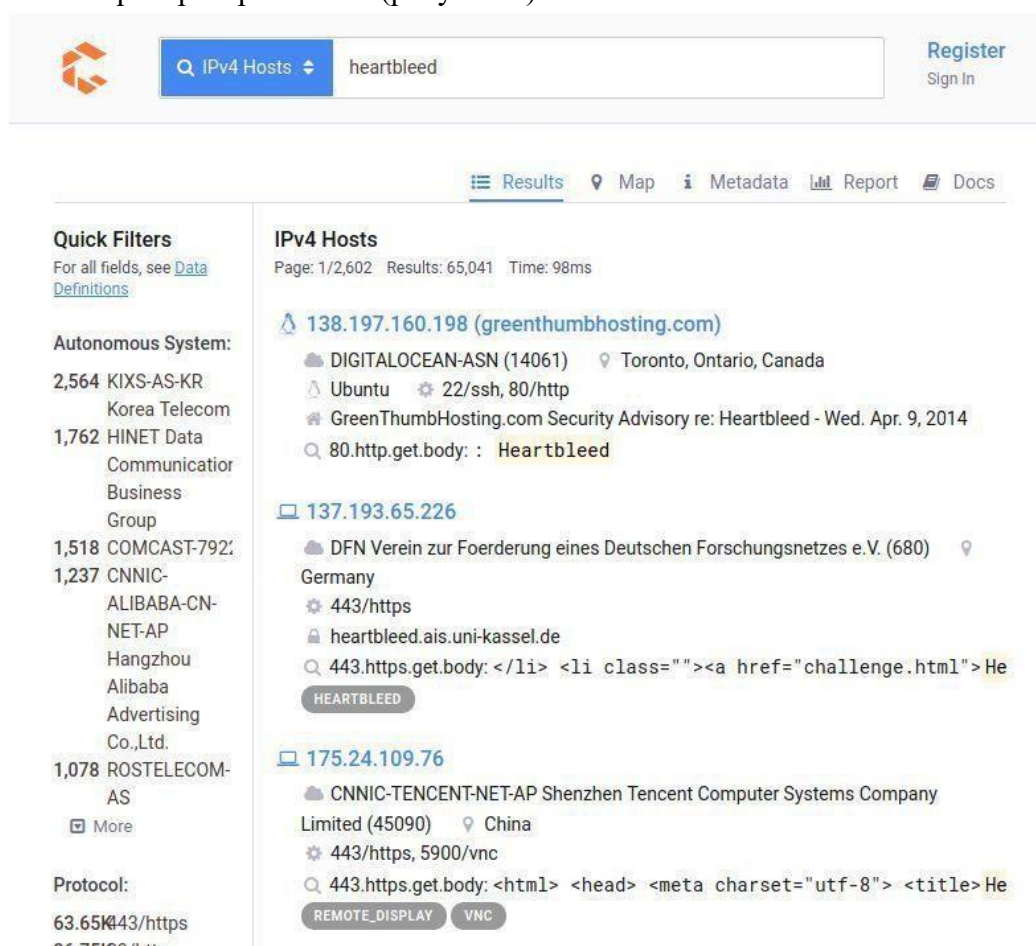


Рисунок 7. Результаты поиска по уязвимостям

Отклики сетевых узлов на запросы Censys помогают идентифицировать ответившие устройства и многое узнать о них. Среди ценной информации: производитель, модель, тип, версия прошивки, открытые порты, активные сервисы и детали о программном обеспечении. Например, использует ли оно шифрование и как именно сконфигурирова-

но. Через Geo IP также можно узнать приблизительное географическое расположение. Вся информация обновляется ежедневно в ходе сканирования общедоступного адресного пространства IPv4 и первого миллиона доменов в рейтинге посещаемости (его ежедневно предоставляет Alexa Internet — дочерняя компания Amazon). Поисковик позволяет экспертам по безопасности оценить распространенность различных уязвимостей.

Censys поддерживает полнотекстовый поиск, логические операторы, условные знаки и фильтры. В общем случае задается искомое слово и опциональные указатели того, где оно должно встречаться. Для фильтрации выдачи можно перечислить порт, протокол, метод, диапазон IP-адресов, географическое положение или ограничения по дате.

Подробный синтаксис представлен в справке и руководстве на сайте <https://search.censys.io/search/language?resource=hosts>.

Для эффективного поиска необходимо указывать поле, в котором хранится атрибут, поэтому необходимо знать поля в наборе данных. С полным списком полей, используемых в Censys, а также типов их значений, можно ознакомиться на вкладке “[Data Definitions](#)” или выбрать просмотр необработанных данных на странице сведений узла.

Для примера можно рассмотреть запрос вида: `80.http.get.headers.www_authenticate: camera` и получим порядка 7 000 результатов камер с веб-интерфейсом. Структура запроса предполагает, что 80 — порт, http — соответствующий ему протокол, get — метод получения данных, header — заголовок, а `www_authenticate: camera` соответствует представлению устройства как камеры.

Как и у Shodan в Censys есть возможность постепенно сужать область поиска, для этого можно зайти в детализацию одного из ответов и посмотреть структуру полей и их значения, чтобы уточнить параметры поиска (рисунок 8).

Host

Attribute	Value
ip	8.8.8.8
location.continent	North America
location.country	United States
location.country_code	US
location.postal_code	
location.timezone	America/Chicago
location.coordinates.latitude	37.751
location.coordinates.longitude	-97.822
location.registered_country	United States
location.registered_country_code	US
location_updated_at	2021-11-26T17:14:23.038540Z
autonomous_system.asn	15169
autonomous_system.description	GOOGLE

Рисунок 8. Детализация запроса в Censys

Помимо этого Censys позволяет делать поиск по местоположению, например, запрос `location.continent: Asia` выдаст все записи об устройствах расположенных в Азии.

Для еще более точного поиска Censys позволяет объединять запросы с использованием логических операторов (and, or ...).

3 Задание

Используя фильтры Shodan найдите устройства на базе Raspbian, расположенные в г. Комсомольске-на-Амуре у которых открыт 80 порт. Сколько устройств из найденных не требуют авторизации?

Используя Censys попробуйте узнать сколько микрокомпьютеров с открытым портом 22 есть в г. Комсомольске-на-Амуре.

8 Материально-техническое обеспечение, необходимое для осуществления образовательного процесса по дисциплине (модулю)

Аудитория	Наименование аудитории (лаборатории)	Используемое оборудование
202/5	Лаборатория безопасности сетей ЭВМ	VipNet Personal FireWall, АРМ с установленной Secret Net Studio 8 системы обнаружения компьютерных атак Выделенные АРМ с установленной Secret Net Studio 8 COB 2 шт. АРМ с установленным Snort, АРМ с установленным WireShark, Анализа сетевого трафика Астра межсетевые экраны: CheckPoint Connectra, Cisco ASA 5505, ЦУС Континент, Secret Net Studio 8, Ноутбук с Windows 7+проектор. 16 ПЭВМ на базе процессоров не ниже Intel Pentium IV

8.1 Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства. Состав программного обеспечения, необходимого для освоения дисциплины, приведен на сайте университета www.knastu.ru / *Наш университет / Образование / 09.04.01 Информатика и вычислительная техника / Рабочий учебный план / Реестр ПО.*

Актуальные на текущий учебный год реквизиты / условия использования программного обеспечения приведены на странице ИТ-управления на сайте университета:
<https://knastu.ru/page/1928>

8.2 Учебно-лабораторное оборудование

Наименование аудитории (лаборатории)	Используемое оборудование
Компьютерный класс	Проектор, персональные ЭВМ с процессорами, с установленным ПО

8.3 Технические и электронные средства обучения

Лекционные занятия (при наличии).

Аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия, тематические иллюстрации).

Лабораторные занятия (при наличии).

Для лабораторных занятий используется аудитория, оснащенная оборудованием, указанным в табл. п. 8.2.

Самостоятельная работа.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде КнАГУ:

- зал электронной информации НТБ КнАГУ;
- компьютерные классы факультета.

9 Иные сведения

Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);
- в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);
- методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);
- выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);
- устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.