МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета

_____ Нестеров П.Н.

20 июня 2023 г.

Рабочая программа дисциплины

Управление информационной безопасностью

Направление подготовки (специальности)
10.04.01 Информационная безопасность

Направленность (профиль)
«Управление информационной безопасностью»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Целью освоения дисциплины «Управление информационной безопасностью» является подготовка к деятельности, связанной с управлением информационной безопасностью, разработкой проектов организационно-распорядительных документов на системы обеспечения информационной безопасности.

Данный курс вырабатывает у студентов знания, навыки и умения организовывать процесс управления информационной безопасностью в объекте информатизации, выявление инцидентов безопасности и меры противодействия возникающим угрозам информационной безопасности.

2. Место дисциплины в структуре ОП

«Управление информационной безопасностью» относится к числу дисциплин обязательной части образовательной программы.

Для успешного усвоения данной дисциплины необходимо, чтобы студент овладел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика» – работа с программными средствами общего назначения;

«Операционные системы» – знание принципов функционирования современных операционных систем и умение их администрировать.

«Вычислительные сети» – знание принципов функционирования вычислительных сетей.

Знания и навыки, полученные в результате изучения дисциплины «Управление информационной безопасностью», используются студентами в дальнейшем при научно-исследовательской работе и в профессиональной деятельности.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Универсальные компетенции		
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**И_УК-1_1** Осуществляет системный анализ задачи, выделяя ее базовые составляющие	**Знать:** - методологию системного подхода при решении задач управления информационной безопасности. **Уметь** - осуществлять классификацию задач и процессов информационной безопасности; - выстраивать процесс обеспечения информационной безопасности. **Владеть** - навыками управления информационной безопасности и анализа последствий при возникновении угроз в сфере информационной безопасности; - навыками критического анализа возникаемых задач информационной безопасности.

	И_УК-1_2 Определяет, интерпретирует и ранжирует информацию, требуемую для решения поставленной задачи	**Знать** - источники угроз и рисков информационной безопасности и их классификацию. **Уметь** - выявлять проблемные ситуации, используя методы управления информационной безопасности; - ранжировать выявленные угрозы информационной безопасности. **Владеть** - навыками устранения выявленных угроз информационной безопасности.
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	**И-УК-3_3** Планирует командную работу, распределяет поручения и делегирует полномочия членам команды.	**Знать:** - основы стратегического планирования работы коллектива для достижения поставленной цели. **Уметь** - планировать командную работу, распределять поручения и делегировать полномочия членам команды. **Владеть** - навыками постановки цели в условиях командой работы; - способами управления командной работой в решении поставленных задач.
Общепрофессиональные компетенции		
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	**И-ОПК-1.5** знает методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности	**Знать:** - основы системного подхода к обеспечению информационной безопасности; - методы оценки рисков, применяемые при управлении информационной безопасностью. **Уметь** - осуществлять классификацию задач и процессов информационной безопасности; - применять методы оценки надежности при управлении информационной безопасностью. **Владеть** - навыками управления информационной безопасностью и анализа последствий при возникновении угроз в сфере информационной безопасности; - навыками использования программных средств, применяемых в управлении информационной безопасностью.
	И-ОПК-1.6 владеть навыками участия в разработке системы обеспечения информационной безопасности	**Знать:** - способы взаимодействия программных средств, участвующих в управлении информационной безопасностью. **Уметь** - разрабатывать и внедрять систему защиты информации; - масштабировать и расширять используемые программные решения, используемые при управлении информационной безопасностью.

	объекта	**Владеть** - навыками планирования и разработки систем информационной безопасности; - навыками оценки используемых программных средств, системы обеспечения информационной безопасности.
ОПК-2 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	**И-ОПК-2_1** Способен осуществлять разработку технического проекта системы (либо ее подсистемы, либо компонента) обеспечения информационной безопасности	**Знать:** - методы управления информационной безопасности. **Уметь** - выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей. **Владеть** - навыками оценки и минимизации рисков при управлении информационной безопасностью; - навыками практической реализации типовых задач исследования
	И-ОПК-2_2 Способен организовать оформление документации технического проекта на систему обеспечения информационной безопасности в соответствии с действующими нормативными документами и государственными стандартами.	**Знать:** - и международные нормативные документы и государственные стандарты по оформлению документации на систему обеспечения информационной безопасности. **Уметь** - проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности **Владеть** - навыками разработки политик безопасности различных уровней.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 акад. часов.

№ п/п	**Темы (разделы) дисциплины, их содержание**	**Семестр**	**Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)**							**Формы текущего контроля успеваемости Форма промежуточной аттестации** ***(по семестрам)***
			Контактная работа							
			лекции	практические	лабораторные	консультации	аттестационные испытания	Самостоятельная работа	контроль	
1	Введение.	2	2	2				8		Опрос на практических занятиях

2	Модель угроз безопасности информации.	2	6	6	8			8		Выполнение лабораторной работы
3	Политики безопасности.	2	6	6	8			8		Выполнение лабораторной работы
4	Аудит информационной безопасности.	2	6	6	8			8		Выполнение лабораторной работы
5	Управление рисками.	2	6	6				8		Опрос на практических занятиях
6	Мониторинг событий безопасности.	2	6	6	8			8		Выполнение лабораторной работы
		2				2	0.5		33.5	Экзамен
	Всего за 2 семестр 180 часов		32	32	32	2	0.5	48	33.5	
	ИТОГО		**32**	**32**	**32**	**2**	**0.5**	**48**	**33.5**	

Содержание разделов дисциплины:

Тема № 1 Введение.

1.1. Цели, критерии и ресурсы управления, эволюция подходов к управлению безопасностью.

1.2. Управление адекватностью и управление рисками.

1.3. Система управления безопасностью, область действия, стратегия построения и внедрения, процессный подход к управлению, задание, идентификация, описание (документирование) и измерение параметров процессов управления безопасностью.

1.4. Цикличность и непрерывность управления – контроль, анализ, планирование, реализация решения.

Тема № 2 Модель угроз безопасности информации.

2.1. Угрозы, атаки и уязвимости, объект и субъект угрозы источник и канал потенциальной реализации угрозы, виды системной классификации угроз.

2.2. Общая методология формирования модели угроз.

2.3. Определение условий создания и процессов использования информационных ресурсов.

2.4. Выявление и идентификация сведений, сопутствующих основным информационным процессам.

Тема № 3 Политики безопасности.

3.1. Понятие политики безопасности. Основные требования, принципы и подходы к разработке политики безопасности, компромисс между защищенностью и производительностью.

3.2. Структура политики информационной безопасности, область действия и цикл жизни политики безопасности, непрерывность и цикличность развития политики безопасности.

3.3. Процесс разработки политики безопасности.

Тема № 4 Аудит информационной безопасности.

4.1. Цели и задачи аудита информационной безопасности в организации.

4.2. Стандарты аудита информационной безопасности.

4.3. Процедура проведения аудита безопасности.

Тема № 5 Управление рисками.

5.1. Анализ рисков. Методы идентификации и оценивания рисков.

5.2. Использование анализа рисков для создания и поддержания политик безопасности.

5.3. Международная практика управления рисками.

Тема № 6 Мониторинг событий безопасности.

6.1. Цели и процедуры мониторинга безопасности.
6.2. Управление инцидентами.
6.3. Реагирование на события и инциденты.
6.4. Расследование инцидентов.

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости)

В процессе осуществления образовательного процесса используются:
программное обеспечение для создания и демонстрации презентаций, иллюстраций и других учебных материалов:
- Microsoft Windows (в составе Microsoft Imagine Premium Electronic Software Delivery);
- Oracle VirtualBox (свободно распространяемое ПО);
- Ubuntu (свободно распространяемое ПО);
- Kali Linux (свободно распространяемое ПО);
- OSSIM (свободно распростаняемое ПО);
- Greenbone Security Manager TRIAL (свободно распространяемое ПО)
- ElasticSearch (свободно распростаняемое ПО).

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

1. Электронная библиотека учебных материалов ЯрГУ:
(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php).

2. Электронно-библиотечная система «Юрайт» https://www.biblio-online.ru/

3. Электронно-библиотечная система «Университетская библиотека online» (www.biblioclub.ru).

4. Новости в сфере информационной безопасности и защиты компьютерной информации журнала «Хакер»: https://xakep.ru/tag/news и журнала «Информационная безопасность»: http://itsec.ru/main.php.

5. Новейшие данные об угрозах работы с подключением к сети Интернет российской компании «Лаборатория Касперского»: http://www.kaspersky.ru/internet-security-center.

6. Федеральный банк данных угроз безопасности, ведущийся в разделе «Техническая защита информации» официального сайта ФСТЭК России (https://bdu.fstec.ru).

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

а) основная литература

1. Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131717.

2. Таненбаум Э. Архитектура компьютера. / Э. Таненбаум; [пер. с англ. Ю. Гороховского, Д. Шинтякова] - 5-е изд. - СПб.: Питер, 2013. - 843 с.

3. Таненбаум Э. Современные операционные системы. / Э. Таненбаум, Х. Бос; [пер. с англ. А. Леонтьевой, М. Малышевой, Н. Вильчинского] - 4-е изд. - СПб.: Питер, 2019. - 1119 с.: ил.

4. Таненбаум Э. Компьютерные сети. / Э. Таненбаум, Д. Уэзеролл; [пер. с англ. А. Гребенькова] - 5-е изд. - СПб.: Питер, 2019. - 955 с.

5. Бирюков А. А. Информационная безопасность: защита и нападение М.: ДМК Пресс, 2017. -434 с.

б) дополнительная литература

1. Белов Е.Б, Лось В.П. и др., «Основы информационной безопасности», Учебное пособие для вузов..- М.: Горячая линия – Телеком, 2006. – 544 с.

2. Девянин П.Н. Модели безопасности компьютерных систем. / П.Н. Девянин - Москва: Академия, 2005. - 320 с.

3. Платонов В. В. Программно-аппаратные средства защиты информации: учебник для вузов. - М.: Академия, 2014. - 331 с.

4. Проскурин В.Г., «Защита программ и данных», 2-е издание, учебное пособие для студ. учреждений высш. проф. образования, М., Издательский центр «Академия», 2012.- 208с

5. Касперски Крис Фундаментальные основы хакерства. Искусство дизассемблирования [Электронный ресурс] / Крис Касперски. — Электрон. текстовые данные. — М. : СОЛОН-ПРЕСС, 2010. — 446 с. — 5-93455-175-2. — Режим доступа: http://www.iprbookshop.ru/65405.html

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

-учебные аудитории для проведения занятий лекционного типа;

-учебные аудитории для проведения практических занятий: лабораторию программно-аппаратных средств обеспечения информационной безопасности;
- учебные аудитории для проведения групповых и индивидуальных консультаций,
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
-помещения для самостоятельной работы;
-помещения для проведения лабораторных занятий.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор:

Доцент кафедры компьютерной безопасности и математических методов обработки информации		А.А. Горохов
должность, ученая степень	*подпись*	*И.О. Фамилия*

Приложение № 1 к рабочей программе дисциплины
«Управление информационной безопасностью»

Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Лабораторная работа №1
(проверка сформированности ОПК-1, индикаторы И-ОПК-1.5 ОПК-1.6)

Пример задания:

Вариант 1

1. Установить виртуальную машину под управлением ОС Microsoft Windows/Linux.
2. Создать пользователей: admin, user, hacker.
3. Для пользователя user создать каталог, содержащий конфиденциальные данные, настроить разграничение доступа, запрещающее доступ пользователей admin и hacker к каталогу.
4. От имени пользователя admin получить доступ к каталогу.
5. Продемонстрировать, что пользователь hacker не имеет возможности получить доступ к каталогу.

Правила выставления оценки по результатам лабораторной работы:

Оценка по результатам самостоятельной работы считается в баллах по следующему принципу: правильно выполненное задание – 2 балла.

Каждое из заданий может быть оценено половиной заявленных по нему баллов, в случае, когда при его выполнении программное обеспечение функционирует, но не взаимодействует с другими компонентами должным образом.

Полностью неправильно выполненное задание – 0 баллов.

Максимальное количество баллов по итогам лабораторной работы – 10 баллов,

Набранное количество баллов от 9-10 соответствует оценке «отлично», 7-8 баллов – оценке «хорошо», 5-6 баллов – оценке «удовлетворительно», менее 5 баллов – оценке «неудовлетворительно» (умения на данном этапе освоения дисциплины не сформированы).

Лабораторная работа №2
(проверка сформированности ОПК-2, индикаторы И_ОПК-2_1, И_ОПК-2_2)

Пример задания:

Вариант 1

1. Для каталога из лабораторной работы №1 настроить правила аудита, позволяющие фиксировать аудит успеха и отказа при доступе к каталогу.
2. Продемонстрировать события журнала при попытках получения доступа пользователем user.
3. Продемонстрировать события журнала при попытках получения доступа пользователем admin.

4. Продемонстрировать события журнала при попытках получения доступа пользователем hacker.
5. Настроить передачу событий на указанный сетевой ресурс.

Правила выставления оценки по результатам лабораторной работы:

Оценка по результатам самостоятельной работы считается в баллах по следующему принципу: правильно выполненное задание – 2 балла.

Каждое из заданий может быть оценено половиной заявленных по нему баллов, в случае, когда при его выполнении программное обеспечение функционирует, но не взаимодействует с другими компонентами должным образом.

Полностью неправильно выполненное задание – 0 баллов.

Максимальное количество баллов по итогам лабораторной работы – 10 баллов,

Набранное количество баллов от 9-10 соответствует оценке «отлично», 7-8 баллов – оценке «хорошо», 5-6 баллов – оценке «удовлетворительно», менее 5 баллов – оценке «неудовлетворительно» (умения на данном этапе освоения дисциплины не сформированы).

Лабораторная работа №3
(проверка сформированности УК-1, индикаторы И_УК-1_1, И_УК-1_2)

Пример задания:

Вариант 1

1. Установить сканер уязвимостей OpenVAS/ Greenbone Security Manager TRIAL.
2. Настроить агентное сканирование для виртуальной машины из лабораторной работы №1.
3. Составить план по устранению выявленных уязвимостей

Правила выставления оценки по результатам лабораторной работы:

Оценка по результатам самостоятельной работы считается в баллах по следующему принципу: правильно выполненное
- задание № 1 – 3 балла;
- задание № 2 – 3 балла;
- задание № 3 – 4 балла.

Каждое из заданий может быть оценено половиной заявленных по нему баллов, в случае, когда при его выполнении программное обеспечение функционирует, но не взаимодействует с другими компонентами должным образом.

Полностью неправильно выполненное задание – 0 баллов.

Максимальное количество баллов по итогам лабораторной работы – 10 баллов,

Набранное количество баллов от 9-10 соответствует оценке «отлично», 7-8 баллов – оценке «хорошо», 5-6 баллов – оценке «удовлетворительно», менее 5 баллов – оценке «неудовлетворительно» (умения на данном этапе освоения дисциплины не сформированы).

Лабораторная работа №4
(проверка сформированности УК-1, индикаторы И_УК-1_1, И_УК-1_2)

Пример задания:

Вариант 1

1. Для предоставленного образа жесткого диска изъять журналы событий операционной системы.

2. Провести анализ журналов событий и других артефактов системы для восстановления хода действий нарушителя.
3. Задокументировать инцидент и предложить рекомендации по устранению последствий инцидента.

Правила выставления оценки по результатам лабораторной работы:

Оценка по результатам самостоятельной работы считается в баллах по следующему принципу: правильно выполненное
- задание № 1 – 3 балла;
- задание № 2 – 3 балла;
- задание № 3 – 4 балла.

Каждое из заданий может быть оценено половиной заявленных по нему баллов, в случае, когда при его выполнении программное обеспечение функционирует, но не взаимодействует с другими компонентами должным образом.

Полностью неправильно выполненное задание – 0 баллов.

Максимальное количество баллов по итогам лабораторной работы – 10 баллов,

Набранное количество баллов от 9-10 соответствует оценке «отлично», 7-8 баллов – оценке «хорошо», 5-6 баллов – оценке «удовлетворительно», менее 5 баллов – оценке «неудовлетворительно» (умения на данном этапе освоения дисциплины не сформированы).

Список заданий к экзамену

На экзамене проверяется сформированность компетенций ОПК-1 (индикаторы ОПК-1.5, ОПК-1.6), ОПК-2 (индикаторы И_ОПК-2_1, И_ОПК-2_2), УК-1 (индикаторы И_УК-1_1, И_УК-1_2), УК-3 (индикатор И_УК-3_3).

Оценка выставляется по результатам экзаменационной работы.

Примеры заданий:

Вариант 1.

1. Для предоставленной виртуальной машины изъять журналы событий операционной системы и другие сведения, необходимые для идентификации инцидента.
2. Провести анализ журналов событий и других артефактов системы для восстановления хода действий нарушителя.
3. Задокументировать инцидент безопасности.
4. Составить проект плана мероприятий по устранению последствий выявленного инцидента информационной безопасности.

Правила выставления оценки по результатам экзаменационной работы:

Оценка по результатам экзаменационной работы считается в баллах по следующему принципу: правильно выполненное
- задание № 1 – 2 балла;
- задание № 2 – 2 балла;
- задание № 3 – 3 балла;
- задание № 4 – 3 балла;

Каждое из заданий может быть оценено половиной заявленных по нему баллов, в случае, когда при его выполнении программное обеспечение функционирует, но не

взаимодействует с другими компонентами должным образом, или в случае, когда команды или описание службы неверно или не полностью задокументированы.

Полностью неправильно выполненное задание – 0 баллов.

Максимальное количество баллов по итогам экзаменационной работы – 10 баллов,

Набранное количество баллов от 9-10 соответствует оценке «отлично», 7-8 баллов – оценке «хорошо», 5-6 баллов – оценке «удовлетворительно», менее 5 баллов – оценке «неудовлетворительно» (умения на данном этапе освоения дисциплины не сформированы).

Приложение № 2 к рабочей программе дисциплины
«Управление информационной безопасностью»

Методические указания для студентов по освоению дисциплины

Основой учебного материала по дисциплине «Управление информационной безопасностью» являются лекционные и практические занятия, источники основной и дополнительной литературы, вместе с Web-материалами, указанными в Рабочей программе и доведенными до студентов (преподавателем и через возможности библиотечного фонда ЯрГУ). По некоторым темам предусмотрены лабораторные занятия, на которых происходит закрепление изученного материала путем применения его к конкретным информационным объектам и отработка навыков работы со специализированным программным обеспечением. Для успешного освоения дисциплины важно углубленное самостоятельное изучение всех тем дисциплины в упомянутых рекомендуемых источниках. Также, в процессе изучения дисциплины, рекомендуется регулярное повторение пройденного практического материала. Материал, представленный в предлагаемой учебной литературе, необходимо еще раз после занятий прорабатывать и, при необходимости, дополнять актуальной информацией, полученной из рекомендованных ресурсов сети «Интернет» и на консультациях и лабораторных занятиях.

Для проверки и контроля усвоения приобретенных практических навыков проводятся мероприятия текущей аттестации в виде лабораторных работ. Также проводятся консультации (при необходимости) по разбору наиболее острых и сложных для усвоения тем, которые вызвали затруднения у студентов.

В конце первого семестра изучения дисциплины студенты сдают экзамен. Экзамен принимается по экзаменационным билетам, каждый из которых включает в себя два три практических вопроса. На самостоятельную подготовку к экзамену выделяется 3 дня.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

Для самостоятельной работы рекомендуется использовать следующую учебную литературу:

1. Таненбаум Э. Архитектура компьютера. / Э. Таненбаум; [пер. с англ. Ю. Гороховского, Д. Шинтякова] - 5-е изд. - СПб.: Питер, 2013. - 843 с.

2. Таненбаум Э. Современные операционные системы. / Э. Таненбаум, Х. Бос; [пер. с англ. А. Леонтьевой, М. Малышевой, Н. Вильчинского] - 4-е изд. - СПб.: Питер, 2019. - 1119 с.: ил.

3. Таненбаум Э. Компьютерные сети. / Э. Таненбаум, Д. Уэзеролл; [пер. с англ. А. Гребенькова] - 5-е изд. - СПб.: Питер, 2019. - 955 с.

4. Бирюков А. А. Информационная безопасность: защита и нападение М.: ДМК Пресс, 2017. -434 с.

Для самостоятельного подбора литературы в библиотеке ЯрГУ рекомендуется использовать:

1. Электронная картотека «Книгообеспеченность» (http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php) раскрывает учебный фонд научной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии книгообеспеченности дисциплин основной и дополнительной литературой, а также цикла дисциплин и специальностей. Электронная картотека «Книгообеспеченность» доступна в сети университета и через Личный кабинет