Федеральное государственное автономное образовательное учреждение высшего образования
«Российский университет дружбы народов имени Патриса Лумумбы»

Факультет физико-математических и естественных наук
(наименование основного учебного подразделения (ОУП)-разработчика ОП ВО)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ПРАКТИКУМ ПО КИБЕРБЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ. ЧАСТЬ 1
(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

38.03.05 БИЗНЕС-ИНФОРМАТИКА
(код и наименование направления подготовки/специальности)

Освоение дисциплины ведется в рамках реализации основной профессиональной образовательной программы высшего образования (ОП ВО):

КИБЕРБЕЗОПАСНОСТЬ В ЭКОНОМИКЕ
(наименование (профиль/специализация) ОП ВО)

2026 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Практикум по кибербезопасности предприятия. Часть 1» входит в программу бакалавриата «Кибербезопасность в экономике» по направлению 38.03.05 «Бизнес-информатика» и изучается в 6 семестре 3 курса. Дисциплину реализует Кафедра теории вероятностей и кибербезопасности. Дисциплина состоит из 4 разделов и 13 тем и направлена на изучение современных методов защиты сетей и обеспечения кибербезопасности в бизнес-информатике.

Целью освоения дисциплины является введение учащихся в предметную область современных методов защиты сетей и обеспечения кибербезопасности в бизнес-информатике. Для достижения поставленной цели выделяются задачи курса: освоение современных методов обеспечения защиты сетей и кибербезопасности предприятия, знакомство слушателей с основами анализа защиты сетей кибербезопасности и выводами, содержанием категорий, используемых в других дисциплинах, связанных с информационными технологиями.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Практикум по кибербезопасности предприятия. Часть 1» направлено на формирование у обучающихся следующих компетенций (части компетенций):

Таблица 2.1. Перечень компетенций, формируемых у обучающихся при освоении дисциплины (результаты освоения дисциплины)

Шифр	**Компетенция**	**Индикаторы достижения компетенции** (в рамках данной дисциплины)
УК-12	Способен: искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач; проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающих информации и данных	УК-12.1 Осуществляет поиск нужных источников информации и данных, воспринимает, анализирует, запоминает и передает информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач; УК-12.2 Проводит оценку информации, ее достоверность, строит логические умозаключения на основании поступающих информации и данных;
ПК-3	Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-3.1 Знает основы архитектуры, устройства и функционирования информационно-вычислительных систем и сетевых подсистем инфокоммуникационной системы организации; основы современных операционных систем; сетевые протоколы; ПК-3.2 Знает основы программирования; современные объектно-ориентированные языки программирования; современные структурные языки программирования; языки современных бизнес-приложений; ПК-3.3 Умеет кодировать на языках программирования; ПК-3.4 Владеет навыками программирования для решения задач профессиональной деятельности;
ПК-5	Владеет навыками организации	ПК-5.1 Знает методы организации управления

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	управления кибербезопасностью предприятий и иных экономических систем	кибербезопасностью предприятий и иных экономических систем; ПК-5.2 Знает основы нормативно-правового регулирования в РФ и иных странах в области защиты информации; ПК-5.3 Умеет применять методы управления кибербезопасностью предприятий и иных экономических систем; ПК-5.4 Умеет использовать нормативно-правовую базу РФ и иных стран в области защиты информации в процессе управления кибербезопасностью предприятий и иных экономических систем; ПК-5.5 Владеет навыками организации управления кибербезопасностью предприятий и иных экономических систем; ПК-5.6 Владеет навыками применения нормативно-правовой базы РФ и иных стран в области защиты информации в процессе управления кибербезопасностью предприятий и иных экономических систем;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Практикум по кибербезопасности предприятия. Часть 1» относится к обязательной части блока 1 «Дисциплины (модули)» образовательной программы высшего образования.

В рамках образовательной программы высшего образования обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Практикум по кибербезопасности предприятия. Часть 1».

Таблица 3.1. Перечень компонентов ОП ВО, способствующих достижению запланированных результатов освоения дисциплины

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
УК-12	Способен: искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач; проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающих информации и данных	Архитектура предприятия и анализ уязвимостей; Цифровая грамотность в информационно-коммуникационных технологиях и бизнесе; Основы использования искусственного интеллекта в информационно-коммуникационных технологиях и бизнесе; Этика использования искусственного интеллекта в информационно-коммуникационных технологиях и бизнесе; Технологии и практика программирования на языке Python для технических специальностей;	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика; Практикум по кибербезопасности предприятия. Часть 2;

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
ПК-3	Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	Основы программирования на Python; Архитектура компьютеров и операционные системы; Объектно-ориентированное моделирование на UML; Основы информационной безопасности;	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика; Кибербезопасность предприятия; Практикум по кибербезопасности предприятия. Часть 2;
ПК-5	Владеет навыками организации управления кибербезопасностью предприятий и иных экономических систем	Экономическая безопасность; Источники угроз кибербезопасности; Технологии обеспечения кибербезопасности предприятий; Противодействие несанкционированным воздействиям в киберпространстве; Бизнес-аналитика и методы принятия решений; Экономика "Умного города" и обеспечение безопасности ее функционирования; Экономическая оценка угроз кибербезопасности;	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика; Технологии распределенного реестра Blockchain; Финансовая безопасность; Практикум по кибербезопасности предприятия. Часть 2; Искусственный интеллект и кибербезопасность;

* - заполняется в соответствии с матрицей компетенций и СУП ОП ВО

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Практикум по кибербезопасности предприятия. Часть 1» составляет «4» зачетные единицы.

Таблица 4.1. Виды учебной работы по периодам освоения образовательной программы высшего образования для очной формы обучения.

Вид учебной работы	**ВСЕГО,** ак.ч.		**Семестр(-ы)**
			6
Контактная работа, ак.ч.	*72*		*72*
Лекции (**ЛК**)	0		0
Лабораторные работы (**ЛР**)	72		72
Практические/семинарские занятия (**СЗ**)	0		0
Самостоятельная работа обучающихся, ак.ч.	*72*		*72*
Контроль (экзамен/зачет с оценкой), ак.ч.	*0*		*0*
Общая трудоемкость дисциплины	**ак.ч.**	***144***	*144*
	зач.ед.	***4***	*4*

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Таблица 5.1. Содержание дисциплины (модуля) по видам учебной работы

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
Раздел 1	Обзор сетевой инфраструктуры.	1.1	Сети, каналы, сетевые протоколы. Сетевое оборудование. Локальные сети предприятия. Семиуровневая модель описания сетевого взаимодействия.	Рассматриваются базовые принципы организации компьютерных сетей: типы сетей, каналы передачи данных, а также сетевые протоколы, определяющие правила обмена информацией между устройствами. Рассматривается основное сетевое оборудование (коммутаторы, маршрутизаторы, концентраторы), необходимое для построения и функционирования сетей. Особое внимание уделено локальным сетям предприятия — их структуре, характеристикам и особенностям эксплуатации в корпоративной среде. Для формализации процессов взаимодействия представлена семиуровневая эталонная модель OSI, которая позволяет детально описать весь путь данных от физической среды до прикладного уровня и облегчает диагностику сетевых проблем.	ЛР
		1.2	Глобальные сети. Социальные сети. Использование сетей в бизнес-процессах.	Рассматриваются глобальные сети (WAN) как основа территориально распределённой связи, включая технологии MPLS, спутниковую связь, протоколы маршрутизации (BGP, OSPF) и защищённые VPN-соединения; анализируются социальные сети в качестве сетевых сервисов с архитектурой клиент-сервер и децентрализованных платформ (ActivityPub, REST API), моделями распространения контента и обработкой больших данных; а также исследуется применение сетей в бизнес-процессах — интеграция ERP/CRM-систем, IP-телефонии, облачных сервисов (SaaS, IaaS), обеспечение качества обслуживания (QoS), непрерывности бизнеса (SLA) и экономической эффективности (TCO, ROI) в условиях объединения локальных и глобальных инфраструктур предприятия. This response is AI-generated, for reference only.	ЛР
		1.3	Участие персонала в социальных сетях. Инструменты воздействия на персонал.	Рассматриваются риски разглашения конфиденциальной информации, снижения продуктивности, а также возможности использования социальных сетей для внутренних	ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				коммуникаций и брендирования. Отдельно исследуются инструменты воздействия на персонал, применяемые как со стороны работодателя (мониторинг активности, политики приемлемого использования, программы обучения, системы мотивации и внутренние корпоративные сети), так и внешние методы влияния (социальная инженерия, таргетированный контент, манипулятивные технологии). Обсуждаются баланс между контролем и доверием, правовые и этические аспекты, а также стратегии защиты персонала от деструктивного информационного воздействия через социальные платформы.	
Раздел 2	Сетевые угрозы. Вредоносные воздействия через сети.	2.1	Вредоносный код (ВК). Угрозы, реализуемые ВК. Распространение ВК через сеть.	Рассматривается вредоносный код (ВК) как программная угроза, реализующая такие виды атак, как перехват данных (снифферы, кейлоггеры), разрушение информации (вирусы, черви, логические бомбы), скрытое управление системами (бэкдоры, руткиты, ботнеты) и вымогательство (шифровальщики). Анализируются основные каналы распространения ВК через сеть: фишинговые письма, заражённые веб-страницы (drive-by download), эксплойты уязвимостей протоколов и сервисов, а также использование съёмных носителей и пиринговых сетей. Особое внимание уделено методам противодействия на сетевом уровне (межсетевые экраны, IDS/IPS, антивирусные шлюзы) и важности своевременного обновления программного обеспечения для предотвращения распространения вредоносного кода.	ЛР
		2.2	Атаки на обслуживание.	Рассматриваются атаки на обслуживание (DoS/DDoS) как класс сетевых воздействий, направленных на нарушение доступности информационных систем путём исчерпания вычислительных ресурсов, пропускной способности каналов или исчерпания лимитов подключений. Анализируются основные типы атак: flood-атаки (ICMP, UDP, SYN-flood), атаки на прикладной уровень (HTTP Slowloris, запросы к БД), амплификационные атаки (DNS, NTP, Memcached) и атаки на уровне протоколов (TCP-десинхронизация). Рассмотрены методы обнаружения и защиты: фильтрация трафика, rate limiting, reverse-прокси, CDN, специализированные анти-DDoS-сервисы, а также роль	ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				сетевого оборудования (firewalls, IDS/IPS, балансировщики нагрузки) в смягчении последствий атак на обслуживание.	
		2.3	Бот сети. Сбор информации через сети.	Рассматриваются ботнеты (сети из заражённых устройств, управляемых злоумышленниками через C&C-серверы с использованием протоколов IRC, HTTP, P2P) как мощный инструмент для проведения распределённых атак (DDoS, рассылка спама, криптомайнинг, кликфрод) и распространения вредоносного кода. Отдельно анализируются методы сбора информации через сети: пассивный сбор (анализ трафика, сниффинг, прослушивание беспроводных каналов), активный сбор (сканирование портов, fingerprinting сервисов, зондирование DNS, SNMP-запросы) и социальная инженерия (фишинг, поддельные точки доступа). Рассмотрены средства противодействия: обнаружение ботнет-активности (анализ аномалий, DNS-блокировки), шифрование трафика (TLS, VPN), контроль доступа, системы обнаружения вторжений (IDS/IPS) и мониторинг сетевой периметрии для предотвращения утечек конфиденциальной информации.	ЛР
Раздел 3	Архитектуры сетевой безопасности.	3.1	Архитектура безопасности семиуровневой модели. ИСО 7498 часть 2.	Рассматривается архитектура безопасности для семиуровневой эталонной модели взаимодействия открытых систем, определяющая общее описание услуг и механизмов защиты информации на всех семи уровнях. Устанавливаются базовые сервисы безопасности и механизмы их реализации с учётом видимых аспектов коммуникационного пути для надёжной передачи данных между оконечными системами. Архитектура расширяет область применения базовой модели, охватывая вопросы защиты обмена данными, при этом не изменяя существующие концепции и принципы. Особое внимание уделяется архитектурным взаимоотношениям средств защиты с эталонной моделью, что обеспечивает согласованный подход к информационной безопасности.	ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
		3.2	Архитектура безопасности сетей в стеке TCP/IP. Протокол IPsec.	Рассматривается архитектура безопасности в стеке протоколов TCP/IP, которая, в отличие от модели OSI, не имеет встроенных на начальном этапе механизмов защиты и реализуется через дополнительные протоколы и расширения. Основное внимание уделяется протоколу IPsec, обеспечивающему защиту на сетевом уровне путём шифрования и аутентификации каждого IP-пакета. Анализируются два основных режима работы IPsec: транспортный (защита полезной нагрузки при сохранении исходного IP-заголовка) и туннельный (полное инкапсулирование пакета с новым заголовком). Рассмотрены ключевые протоколы IPsec: AH (аутентификация заголовка и целостность данных), ESP (шифрование, аутентификация и защита от повторов), а также IKE для автоматического управления криптографическими ключами. Описываются варианты применения IPsec для организации VPN, защиты межсетевых взаимодействий и обеспечения конфиденциальности, целостности и доступности данных при передаче по открытым сетям.	ЛР
		3.3	Протоколы сетевой аутентификации. VPN. Инфраструктура открытых ключей.	Рассматриваются протоколы сетевой аутентификации (RADIUS, Diameter, Kerberos, EAP), обеспечивающие проверку подлинности пользователей и устройств при доступе к сетевым ресурсам, а также технологии VPN (IPsec, OpenVPN, WireGuard, SSL/TLS), создающие защищённые туннели поверх открытых сетей с шифрованием и инкапсуляцией трафика. Отдельное внимание уделяется инфраструктуре открытых ключей (PKI), включающей центры сертификации, списки отзыва сертификатов и системы управления ключами, которая лежит в основе доверенного обмена ключами, цифровых подписей и аутентификации в протоколах TLS, IPsec и VPN-решениях. Анализируется взаимосвязь этих компонентов: PKI обеспечивает криптографическую основу для безопасной аутентификации и установки VPN-соединений, что в совокупности позволяет строить защищённые корпоративные	ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				сети с контролируемым удалённым доступом.	
Раздел 4	Механизмы защиты предприятия от сетевых атак.	4.1	Системы обнаружения вторжений. IDS, SIEM	Рассматриваются системы обнаружения вторжений (IDS), классифицируемые по способу мониторинга (сетевые NIDS и хостовые HIDS) и методу анализа (сигнатурный, основанный на правилах, и аномалийный, выявляющий отклонения от нормального поведения), а также платформы SIEM, обеспечивающие централизованный сбор, корреляцию событий и анализ логов от различных сетевых устройств, серверов и приложений для выявления комплексных атак и инцидентов безопасности. Анализируются принципы работы IDS — перехват и анализ трафика, генерация при совпадении с сигнатурами или аномалиями, а также функциональность SIEM: нормализация событий, корреляция по временным и пространственным признакам, построение дашбордов и автоматическое реагирование. Описываются различия между активными (IPS) и пассивными системами, роль SIEM в управлении инцидентами и соответствии регуляторным требованиям, а также ограничения (ложные срабатывания, необходимость настройки, шифрованный трафик).	ЛР
		4.2	Межсетевые экраны.	Рассматриваются межсетевые экраны как ключевое средство контроля сетевого доступа, осуществляющее фильтрацию трафика на основе заданных правил. Анализируются основные типы: пакетные фильтры (анализ заголовков IP/портов), stateful-экраны (отслеживание состояния соединений), прокси-серверы (прикладной уровень с глубокой инспекцией) и межсетевые экраны нового поколения (NGFW), объединяющие фильтрацию с системами предотвращения вторжений (IPS), распознаванием приложений и анализом содержимого. Рассматриваются принципы построения правил фильтрации по протоколам, адресам, портам и контексту соединения, а также методы организации зон безопасности (внутренняя, демилитаризованная зона, внешняя сеть). Описываются сценарии применения — защита периметра, сегментация внутренних сетей, контроль доступа удалённых пользователей	ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				(VPN) и ограничение исходящего трафика.	
		4.3	Антивирусы. Демилитаризованная зона. DMZ.	Рассматриваются антивирусные средства как программные или программно-аппаратные решения для обнаружения, блокировки и удаления вредоносного кода с использованием сигнатурного, эвристического и поведенческого анализа, а также демилитаризованная зона (DMZ) — сегмент сети, изолированный между внутренней корпоративной сетью и внешней (обычно интернет) для размещения общедоступных сервисов (веб-серверы, почтовые шлюзы, прокси) с ограниченным доступом извне и строгим контролем трафика через межсетевые экраны. Анализируется взаимосвязь этих компонентов: антивирусная защита применяется как на конечных устройствах внутри сети, так и на шлюзах в DMZ для предотвращения проникновения угроз через публичные сервисы, тогда как DMZ снижает риск распространения атак с скомпрометированных внешних серверов во внутреннюю сеть. Рассматриваются типовые конфигурации DMZ с одним или двумя межсетевыми экранами, принципы минимальных привилегий и роль антивирусной проверки трафика HTTP, SMTP и FTP, проходящего через демилитаризованную зону.	ЛР
		4.4	Прокси-серверы.	Рассматриваются прокси-серверы как промежуточные шлюзы между клиентами и целевыми серверами, выполняющие функции перенаправления запросов, фильтрации трафика, кэширования контента, анонимизации (скрытие реального IP-адреса клиента) и контроля доступа к веб-ресурсам. Анализируются основные типы: прямые (forward proxy) для выхода клиентов в интернет, обратные (reverse proxy) для балансировки нагрузки и защиты веб-серверов, прозрачные (transparent proxy), работающие без настройки на стороне клиента, и анонимные прокси, изменяющие заголовки для сокрытия информации о запросе. Рассматриваются сценарии применения — организация корпоративной фильтрации	ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				интернет-трафика (черные списки, контентная фильтрация), ускорение загрузки через кэширование, обеспечение анонимности, обход географических блокировок и защита внутренней инфраструктуры от прямых внешних запросов. Описываются ограничения (отсутствие сквозного шифрования при работе с HTTP, необходимость аутентификации) и отличия от VPN и межсетевых экранов.	

* - заполняется только по **ОЧНОЙ** форме обучения: *ЛК – лекции; ЛР – лабораторные работы; СЗ – практические/семинарские занятия.*

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Таблица 6.1. Материально-техническое обеспечение дисциплины

Тип аудитории	**Оснащение аудитории**	**Специализированное учебное/лабораторное оборудование, ПО и материалы для освоения дисциплины (при необходимости)**
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами (в количестве ____ шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams или аналог. Дополнительное ПО: офисный пакет MS Office или LibreOffice.
Для самостоятельной работы	Аудитория для самостоятельной работы обучающихся (может использоваться для проведения семинарских занятий и консультаций), оснащенная комплектом специализированной мебели и компьютерами с доступом в ЭИОС.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams или аналог. Дополнительное ПО: офисный пакет MS Office или LibreOffice.

* - аудитория для самостоятельной работы обучающихся указывается **ОБЯЗАТЕЛЬНО**!

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Грушо Александр Александрович. Защита сетей и кибербезопасность : учебное пособие / А.А. Грушо, Е.Е. Тимонина, В.А. Бесчастный. - Электронные текстовые данные. - Москва : РУДН, 2023. - 88 с. : ил.
URL: https://lib.rudn.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=515837&idb=0

2. Внуков А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277

3. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490019

Дополнительная литература:

1. Внуков, А. А. Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный //

Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490278

2. Грекул, В. И. Проектирование информационных систем: учебник и практикум для вузов / В. И. Грекул, Н. Л. Коровкина, Г. А. Левочкина. — Москва : Издательство Юрайт, 2022. — 385 с. — (Высшее образование). — ISBN 978-5-9916-8764-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489918

3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491249

4. Казарин О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493262

Ресурсы информационно-телекоммуникационной сети «Интернет»:

1. ЭБС РУДН и сторонние ЭБС, к которым студенты университета имеют доступ на основании заключенных договоров

- Электронно-библиотечная система РУДН – ЭБС РУДН http://lib.rudn.ru/MegaPro/Web
- ЭБС «Университетская библиотека онлайн» http://www.biblioclub.ru
- ЭБС Юрайт http://www.biblio-online.ru
- ЭБС «Консультант студента» www.studentlibrary.ru
- ЭБС «Троицкий мост»

2. Базы данных и поисковые системы

- электронный фонд правовой и нормативно-технической документации http://docs.cntd.ru/
- поисковая система Яндекс https://www.yandex.ru/
- поисковая система Google https://www.google.ru/
- реферативная база данных SCOPUS http://www.elsevierscience.ru/products/scopus/

Учебно-методические материалы для самостоятельной работы обучающихся при освоении дисциплины/модуля:*

1. Курс лекций по дисциплине «Практикум по кибербезопасности предприятия. Часть 1».

* - все учебно-методические материалы для самостоятельной работы обучающихся размещаются в соответствии с действующим порядком на странице дисциплины **в ТУИС**!

РАЗРАБОТЧИК:

Доцент кафедры теории вероятностей и кибербезопасности		Бесчастный Виталий Александрович
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой теории вероятностей и кибербезопасности		Самуйлов Константин Евгеньевич
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой теории вероятностей и кибербезопасности		Самуйлов Константин Евгеньевич
Должность, БУП	*Подпись*	*Фамилия И.О.*