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 2
(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 2» входит в программу бакалавриата «Кибербезопасность в экономике» по направлению 38.03.05 «Бизнес-информатика» и изучается в 7 семестре 4 курса. Дисциплину реализует Кафедра теории вероятностей и кибербезопасности. Дисциплина состоит из 3 разделов и 11 тем и направлена на изучение современной архитектуры предприятия и анализа его уязвимостей в бизнес-информатике.

Целью освоения дисциплины является введение учащихся в предметную область современной архитектуры предприятия и анализа его уязвимостей в бизнес-информатике. Для достижения поставленной цели выделяются задачи курса: освоение современных методов анализа архитектуры предприятия, знакомство слушателей с основными алгоритмами выявления уязвимостей предприятия 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 2» 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 управления	ПК-5.1 Знает методы организации управления кибербезопасностью предприятий и иных экономических

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	кибербезопасностью предприятий и иных экономических систем	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 2» 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 2».

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	Основы анализа данных в машинном обучении; 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; Практикум по кибербезопасности предприятия. Часть 1; Технологии и практика программирования на языке Python для технических	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика;

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
		специальностей; Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы);	
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; Практикум по кибербезопасности предприятия. Часть 1;	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика;
ПК-5	Владеет навыками организации управления кибербезопасностью предприятий и иных экономических систем	Практикум по кибербезопасности предприятия. Часть 1; Экономическая безопасность; Цифровая трансформация глобальной экономики; Источники угроз кибербезопасности; Технологии обеспечения кибербезопасности предприятий; Противодействие несанкционированным воздействиям в киберпространстве; Анализ и показатели эффективности кибербезопасности предприятия; Экономическая оценка угроз кибербезопасности; Бизнес-аналитика и методы принятия решений; Экономика "Умного города" и обеспечение безопасности ее функционирования; Кибербезопасность платежных систем;	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика;

* - 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 2» 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)**
			7
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	Инвентаризация бизнес процессов предприятия.	1.1	Объекты предприятия, подлежащие защите. Субъекты влияющие на защищенность. Функциональная модель предприятия. Организационная модель предприятия. Модель внешних взаимодействий предприятия. Бизнес процессы предприятия.	Рассматриваются объекты предприятия, подлежащие защите (информационные активы, технические средства, программное обеспечение, каналы связи, персонал и инфраструктура), а также субъекты, влияющие на защищённость (внутренние — сотрудники, администраторы, руководство, и внешние — злоумышленники, конкуренты, регулирующие органы, поставщики услуг). Анализируются функциональная модель предприятия (совокупность бизнес-функций и взаимосвязей между ними), организационная модель (структура управления, подчинения, роли и зоны ответственности), модель внешних взаимодействий (контрагенты, государственные органы, партнёры, клиенты и каналы связи с ними) и бизнес-процессы предприятия (последовательности действий, создающих ценность, включая основные, обеспечивающие и управляющие процессы). Показано, что эффективная защита предприятия строится на взаимосвязанном анализе всех перечисленных моделей: выявление критичных объектов требует понимания бизнес-процессов, организационная модель определяет разграничение доступа, функциональная модель — уязвимости на стыках функций, а модель внешних взаимодействий — угрозы, приходящие извне.	ЛР
		1.2	Информационные технологии. Информационная модель предприятия. Модель информационных потоков предприятия. Информационные системы предприятия.	Рассматриваются информационные технологии как совокупность методов, процессов и средств сбора, обработки, хранения и передачи данных, лежащих в основе автоматизации деятельности предприятия, а также информационная модель предприятия — формализованное описание сущностей (объектов, атрибутов, связей) и правил их изменения, отражающее семантику предметной области. Анализируется модель информационных потоков предприятия, определяющая направления, интенсивность, форматы и регламенты движения данных между подразделениями, информационными системами и внешними контрагентами, включая документооборот, запросы и отчёты. Рассматриваются	ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				информационные системы предприятия (ERP, CRM, SCM, BI, ECM, и др.) как программно-аппаратные комплексы, реализующие сбор, хранение и обработку информации в соответствии с бизнес-процессами, а также взаимосвязь перечисленных моделей: информационная модель является концептуальной основой для проектирования баз данных и потоков, а информационные системы выступают технологической реализацией этих моделей, обеспечивая целостность, доступность и защищённость данных.	
		1.3	Активы предприятия и их классификация.	Рассматриваются активы предприятия как все ресурсы, имеющие ценность для организации и подлежащие защите, включая материальные (оборудование, здания, носители), нематериальные (интеллектуальная собственность, репутация, лицензии), информационные (базы данных, документация, конфиденциальные сведения) и кадровые (знания, навыки сотрудников). Анализируются основные классификации активов: по форме существования (материальные/нематериальные), по степени критичности (высокая, средняя, низкая), по принадлежности (собственные, арендованные), по месту размещения (локальные, облачные, у подрядчиков), по юридическому статусу (с ограничениями доступа, открытые), а также по процессам, в которых они участвуют (основные, вспомогательные, управленческие). Отмечается, что классификация активов является основой для построения системы управления рисками, определения приоритетов защиты, назначения владельцев активов и выбора адекватных мер безопасности.	ЛР
		1.4	Нормативные документы предприятия.	Рассматриваются нормативные документы предприятия как совокупность внутренних регламентов, политик, стандартов, инструкций и положений, определяющих порядок функционирования, управления, информационной безопасности и взаимодействия между подразделениями и	ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				сотрудниками. Анализируется их классификация по уровню обязательности (политики высшего уровня, процедуры, рабочие инструкции), по сфере действия (общеорганизационные, технологические, кадровые, финансовые), по отношению к внешним требованиям (реализующие законодательство, отраслевые стандарты и договорные обязательства). Описываются ключевые документы в области защиты информации (политика информационной безопасности, регламенты разграничения доступа, план непрерывности бизнеса, инструкции по реагированию на инциденты), а также взаимосвязь нормативной базы с организационной моделью, бизнес-процессами и системой управления рисками предприятия.	
Раздел 2	Анализ архитектуры предприятия и потенциальных ущербов.	2.1	Использование активов в бизнес процессах. Доступы к активам предприятия. Реализация политики доступов. Использование модели информационных потоков для анализа взаимодействий функциональной модели и организационной модели предприятия.	Рассматривается использование активов предприятия в бизнес-процессах (закрепление активов за конкретными процессами и владельцами, определение ценности и критичности), управление доступами к активам на основе принципов минимальных привилегий и разделения обязанностей, а также реализация политики доступов через ролевые модели (RBAC), мандатные метки (MAC) или дискреционные списки (DAC) с применением средств аутентификации и авторизации. Отдельное внимание уделяется использованию модели информационных потоков для анализа взаимодействий функциональной модели (что делается) и организационной модели (кто делает): сопоставление потоков данных с функциями и ролями позволяет выявить избыточные доступы, пересечения полномочий, конфликтные транзакции и потенциальные каналы утечек, что служит основой для корректного проектирования систем контроля доступа и минимизации рисков нарушения целостности и конфиденциальности активов.	ЛР
		2.2	Ответственность за целостность	Рассматриваются вопросы ответственности за целостность	ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
			информационных потоков и точки разрывов ответственности. Участие внешних акторов в бизнес процессах предприятия. Возможные ущербы активам предприятия.	информационных потоков (закрепление обязанностей за владельцами процессов, администраторами и пользователями), а также точки разрывов ответственности — места на стыках подразделений, систем или этапов бизнес-процесса, где контроль над данными временно утрачивается или передаётся между разными субъектами, что создаёт риски искажения, потери или несанкционированной модификации информации. Анализируется участие внешних акторов (контрагентов, аутсорсеров, регуляторов, клиентов) в бизнес-процессах предприятия, что вносит дополнительные угрозы из-за различий в политиках безопасности, уровнях доверия и технических средствах защиты. Описываются возможные ущербы активам предприятия: нарушение конфиденциальности (утечка данных), целостности (подмена или уничтожение), доступности (блокирование работы сервисов), а также прямые финансовые потери, репутационный вред, штрафы регуляторов и нарушение непрерывности бизнес-процессов.	
		2.3	Структура ответственности за использование активов. Отражение ответственности в нормативных документах.	Рассматривается структура ответственности за использование активов, включающая распределение ролей (владельцы активов, назначенные пользователи, администраторы безопасности, руководство) с закреплением прав, обязанностей и мер дисциплинарной ответственности за нарушение правил обращения с активами. Анализируется отражение этой ответственности в нормативных документах предприятия: политиках информационной безопасности, положениях о подразделениях, должностных инструкциях, регламентах доступа и соглашениях о неразглашении, где фиксируются зоны ответственности, порядок отчётности, санкции за нарушения и процедуры контроля. Показано, что формальное документирование структуры ответственности позволяет избежать разрывов в управлении активами, обеспечить подотчётность и служит основой для аудита и расследования инцидентов.	ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
		2.4	Инструменты реализаций политик и обеспечения ответственности.	Рассматриваются инструменты реализации политик и обеспечения ответственности, включая организационные (регламенты, должностные инструкции, соглашения о неразглашении, процедуры аудита и расследований) и технические средства (системы управления доступом, средства мониторинга и логирования, SIEM, DLP-системы, цифровые подписи, журналы аудита). Анализируется применение этих инструментов для автоматического контроля соблюдения политик, фиксации действий с активами, назначения и отслеживания ответственности, а также для доказательной базы при нарушениях. Показано, что сочетание организационных мер с техническими средствами обеспечивает непрерывный цикл управления доступом, подотчётности и принуждения к исполнению политик безопасности.	ЛР
Раздел 3	Анализ уязвимостей.	3.1	Уязвимости, связанные с утечками ценной информации.	Рассматриваются уязвимости, связанные с утечками ценной информации, включая технические (незащищённые каналы связи, отсутствие шифрования, уязвимости протоколов и ПО, неконтролируемые съёмные носители, скрытые каналы передачи данных), организационные (слабые политики доступа, отсутствие сегментации сети, недостаточный контроль привилегий, неформальное общение сотрудников) и человеческие (социальная инженерия, фишинг, неосторожные действия персонала, использование неавторизованных сервисов). Анализируются типовые векторы утечек: перехват трафика, несанкционированный доступ к базам данных, отправка данных через веб-интерфейсы и мессенджеры, компрометация учётных записей, а также методы снижения рисков (шифрование, DLP-системы, мониторинг потоков, обучение персонала).	ЛР
		3.2	Уязвимости, связанные с целостностью информации и инфраструктуры	Рассматриваются уязвимости, связанные с целостностью информации и инфраструктуры предприятия	ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
			предприятия. Уязвимости, связанные с доступностью информации и ресурсов.	(несанкционированное изменение, подмена, вставка или удаление данных, атаки на системы контроля версий, компрометация обновлений ПО, повреждение журналов аудита, перехват и модификация трафика без обнаружения, отсутствие механизмов электронной подписи и контроля хешей), а также уязвимости, связанные с доступностью информации и ресурсов (отказы оборудования, перегрузка каналов и серверов (DoS/DDoS), программные сбои, ошибки конфигурации, отсутствие резервирования и планов непрерывности, единые точки отказа, атаки на DNS и маршрутизацию, а также организационные проблемы, такие как недостаточный контроль доступа к критическим узлам или отсутствие аварийного электропитания). Показано, что снижение этих рисков требует комплексного подхода, включающего резервное копирование, контроль целостности (контрольные суммы, системы HIDS), избыточность компонентов, сегментацию сети и формализованные процедуры реагирования на инциденты.	
		3.3	Уязвимости, связанные устойчивостью бизнес процессов к сбоям и ошибкам. Уязвимости, связанные с внешними взаимодействиями.	Рассматриваются уязвимости, связанные с устойчивостью бизнес-процессов к сбоям и ошибкам (отсутствие резервирования критических узлов, жёсткие последовательности операций без точек восстановления, неформализованные ручные действия, ошибки в настройках интеграций, недостаточное тестирование сценариев отказов, отсутствие механизмов автоматического переключения и временных буферов), а также уязвимости, связанные с внешними взаимодействиями (зависимость от надёжности контрагентов и поставщиков услуг, незащищённые каналы обмена данными, отсутствие контроля исполнения договорных обязательств по безопасности, риски через стороннее ПО и API, использование внешних облачных сервисов без формальных SLA, утечки через партнёрские сети и подрядчиков). Показано, что снижение данных уязвимостей требует построения устойчивых бизнес-процессов с резервированием, регулярным	ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				тестированием на отказоустойчивость, а также управления внешними рисками через аудит контрагентов, соглашения об уровне услуг и защиту границ взаимодействия.	

* - 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 20 шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	ОС Linux/Windows, браузер, киберполигон Ampire, Wireshark. Дополнительное ПО: офисный пакет MS Office или LibreOffice, OBS Studio
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.	ОС Linux/Windows, браузер, киберполигон Ampire, Wireshark. Дополнительное ПО: офисный пакет MS Office или LibreOffice, OBS Studio

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Зараменских Е. П. Архитектура предприятия : учебник для вузов / Е. П. Зараменских, Д. В. Кудрявцев, М. Ю. Арзуманян ; под редакцией Е. П. Зараменских. — Москва : Издательство Юрайт, 2022. — 410 с. — (Высшее образование). — ISBN 978-5-534-06712-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493118

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

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. Полякова Т. А. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2022. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498889

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 https://mega.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 «Знаниум» https://znanium.ru/

2. Базы данных и поисковые системы

- Sage https://journals.sagepub.com/
- Springer Nature Link https://link.springer.com/
- Wiley Journal Database https://onlinelibrary.wiley.com/
- Наукометрическая база данных Lens.org https://www.lens.org

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

1. Курс лекций по дисциплине «Практикум по кибербезопасности предприятия. Часть 2».

* - 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.*