Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Проректор по учебной работе

_____ С.Т. Князев
«23» _____ 2019 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Модуль	Код модуля
Проектный интенсив ВС – «Информационное обеспечение национальной безопасности»	1147777

Екатеринбург, 2019

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа Правовое обеспечение национальной безопасности	**Код ОП** 40.05.01/33.01
Направление подготовки Правовое обеспечение национальной безопасности	**Код направления и уровня подготовки** 40.05.01

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Крылов Виктор Гаврилович	-	Старший преподаватель	Кафедра региональной экономики, инновационного предпринимательства и безопасности

Руководитель модуля В.Г. Крылов

Рекомендовано учебно-методическим советом Института государственного управления и предпринимательства

Протокол № 10 от 26 июня 2019г.

Согласовано:

Дирекция образовательных программ Р. Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Проектный интенсив ВС - Информационное обеспечение национальной безопасности

1.1. Аннотация содержания модуля

В состав модуля Проектный интенсив ВС - «Информационное обеспечение национальной безопасности» входит одна дисциплина «Информационное обеспечение национальной безопасности» - проект ВС.

Модуль направлен на выработку у студентов базовых профессиональных умений и навыков в области информационных технологий для анализа информации и поддержки принятия управленческих решений, технологии защиты информации, web-технологии, технологии управления проектами и работы со специализированным прикладным программным обеспечением при ведении управленческой деятельности.

Модуль представляет собой основу для вовлечения студентов в проектную деятельность в области информационной безопасности и сопряжен с реализацией одноименных проектного практикума и проектного интенсива.

Модуль является практико-ориентированным. Освоение учебного материала по каждому разделу будет осуществляться студентами под руководством специалистов Института экономики и управления. Максимальный акцент в освоении дисциплины сделан на отработке практических умений посредством деловых и ролевых игр, тренингов, использовании кейс-метода.

Экзамен по модулю проводится в форме представления и защиты студентами групповых проектов, выполняемых на протяжении семестра изучения модуля, на основе подготовленных презентаций. Критерии оценки включают в себя содержательную проработанность проекта по темам основных разделов модуля и выразительность инфографики, представленной в презентации. Оценка выставляется методом взаимооценки презентаций студентами под руководством преподавателя.

Дисциплина занимает важное место в структуре образования и подготовки будущих специалистов экономической безопасности. Теоретической основой дисциплины являются основные положения дисциплин математики и информатики в объемах базовых курсов.

1.2. Структура и объем модуля, распределение объема времени по видам учебной работы по дисциплинам модуля

Таблица 1

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах и часах	Форма итоговой промежуточной аттестации по дисциплинам модуля и в целом по модулю
1.	«Информационное обеспечение национальной безопасности» - проект ВС	6 з.е./216 час.	Экзамен
	ИТОГО по модулю:	6 з.е./216 час.	Экзамен

1.3. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	*Экономическая и финансовая безопасность государства*
Постреквизиты и корреквизиты модуля	*Правовое обеспечение внутренней безопасности государства*

1.4. Распределение компетенций по дисциплинам модуля, планируемые результаты обучения (индикаторы) по модулю

Изучение дисциплин модуля предусматривает формирование компетенций посредством последовательного освоения результатов обучения на определенном уровне сложности содержания.

Результаты обучения по дисциплине – это конкретные знания, умения, опыт и другие результаты (содержательные компоненты компетенций), которых планируется достичь на этапе изучения дисциплины модуля и которые должны будут продемонстрированы обучающимися и оценены преподавателем по индикаторам/измеряемым критериям, включенным в формулировку результатов обучения.

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины.

Индикаторы должны учитываться при выборе и составлении заданий контрольно-оценочных мероприятий (оценочных средств) текущей и промежуточной аттестации.

Таблица 2

Перечень дисциплин модуля	**Код и наименование компетенции**	**Планируемые результаты обучения (индикаторы)**
1	2	3
«Информационное обеспечение национальной безопасности» проект ВС	УК-3. Способен организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.	**Знать**: • понятие эффективной команды, процесс ее создания и правила работы в команде; • правила распределения ролей в команде; • правила принятия решений в команде; • способы взаимодействия членов команды. **Уметь**: • характеризовать понятие эффективной команды, процесс ее создания и правила работы в команде**;** • определять свою роль в процессе принятия групповых или командных решений с учетом собственных личностных ресурсов и ресурсов участников команды; • в процессе принятия командного решения выполнять предписанные командные роли и осуществлять продуктивное взаимодействие с участниками команды с учетом особенностей их поведения и интересов;

		• проявлять гибкость и адаптивность мышления в межличностном взаимодействии; • демонстрировать развитую речь, умение слушать и убеждать. **Практический опыт, владение:** • навыками распределения задач в команде; • навыками организации командного взаимодействия; • навыками убеждения и взаимодействия с членами команды; • навыками оценки эффективности работы команды и отдельных ее членов.
	ПК-8. Способен соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности	В результате освоения дисциплины студент должен: **Знать:** • законодательство Российской Федерации в сфере обеспечения информационной безопасности; • основные требования к сбору, распространению, обработке и защите информации, работе с персональными данными; • правовое регулирование в области защиты государственной тайны; • меры ответственности за нарушения законодательства в сфере защиты государственной тайны и информационной безопасности. **Уметь:** • определять применимые нормативные акты в сфере обеспечения информационной безопасности; • толковать и применять релевантные нормы в сфере обеспечения информационной безопасности; • устанавливать соответствие фактических обстоятельств основным требованиям к сбору, распространению, обработке и защите информации, работе с персональными данными; • применять нормативные акты в области защиты государственной тайны; • определять надлежащие меры ответственности за нарушения законодательства в сфере защиты государственной тайны и информационной безопасности. **Практический опыт, владение:** • навыками определения применимых нормативных актов в сфере обеспечения информационной безопасности; • навыками толкования и применения релевантных норм в сфере обеспечения информационной безопасности; • навыками установления соответствия

		фактических обстоятельств основным требованиям к сбору, распространению, обработке и защите информации, работе с персональными данными; • навыками применения нормативных актов в области защиты государственной тайны; • навыками определения надлежащих мер ответственности за нарушения законодательства в сфере защиты государственной тайны и информационной безопасности.
	ПК-10. Способен принимать адекватные и соответствующие законодательству и ситуации управленческие решения в целях обеспечения национальной безопасности.	В результате освоения дисциплины студент должен: **Знать:** • основные угрозы безопасности при использовании информационных технологий; • меры ответственности за нарушение информационной безопасности; • назначение различных средств и систем защиты информации; • средства безопасности современных операционных систем; • способы защиты информации; • основы криптографических мер защиты информации; • организационные меры по защите информации. **Уметь:** • определять основные угрозы безопасности при использовании информационных технологий; • производить мониторинг безопасности информационных систем; • применить полученные знания в процессе дальнейшего обучения и своей профессиональной деятельности. **Практический опыт, владение:** • навыками выявления нарушений информационной безопасности; • навыками работы со встроенными средствами безопасности операционных систем и офисного программного обеспечения; навыками безопасной работы в глобальных и локальных информационных сетях.

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной форме.

2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАЗДЕЛ 2. ПРОГРАММЫ МОДУЛЯ

ПРОЕКТНЫЙ ИНТЕНСИВ ВС – «ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ 1

«ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ» - ПРОЕКТ ВС

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Крылов Виктор Гаврилович	-	Ст. преподаватель	Региональной экономики, инновационного предпринимательства и безопасности

Рекомендовано учебно-методическим советом института государственного управления и предпринимательства

Протокол № 10 от 26 июня 2019г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 1 «Информационное обеспечение национальной безопасности» проект ВС

1.1. Технологии обучения, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучения.

о Базовый уровень.

1.2. Планируемые результаты обучения (индикаторы) по дисциплине

Таблица 1.2

Код и наименование компетенции	Планируемые результаты обучения (индикаторы)
УК-3. Способен организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.	**Знать**: • понятие эффективной команды, процесс ее создания и правила работы в команде; • правила распределения ролей в команде; • правила принятия решений в команде; • способы взаимодействия членов команды. **Уметь**: • характеризовать понятие эффективной команды, процесс ее создания и правила работы в команде**;** • определять свою роль в процессе принятия групповых или командных решений с учетом собственных личностных ресурсов и ресурсов участников команды; • в процессе принятия командного решения выполнять предписанные командные роли и осуществлять продуктивное взаимодействие с участниками команды с учетом особенностей их поведения и интересов; • проявлять гибкость и адаптивность мышления в межличностном взаимодействии; • демонстрировать развитую речь, умение слушать и убеждать. **Практический опыт, владение**: • навыками распределения задач в команде; • навыками организации командного взаимодействия; • навыками убеждения и взаимодействия с членами команды • навыками оценки эффективности работы команды и отдельных ее членов.
ПК-8. Способен соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности	В результате освоения дисциплины студент должен: **Знать:** • законодательство Российской Федерации в сфере обеспечения информационной безопасности; • основные требования к сбору, распространению, обработке и защите информации, работе с персональными данными; • правовое регулирование в области защиты государственной тайны; • меры ответственности за нарушения законодательства в сфере защиты государственной тайны и информационной безопасности. **Уметь:** • определять применимые нормативные акты в сфере обеспечения информационной безопасности;

	• толковать и применять релевантные нормы в сфере обеспечения информационной безопасности; • устанавливать соответствие фактических обстоятельств основным требованиям к сбору, распространению, обработке и защите информации, работе с персональными данными; • применять нормативные акты в области защиты государственной тайны; • определять надлежащие меры ответственности за нарушения законодательства в сфере защиты государственной тайны и информационной безопасности. **Практический опыт, владение:** • навыками определения применимых нормативных актов в сфере обеспечения информационной безопасности; • навыками толкования и применения релевантных норм в сфере обеспечения информационной безопасности; • навыками установления соответствия фактических обстоятельств основным требованиям к сбору, распространению, обработке и защите информации, работе с персональными данными; • навыками применения нормативных актов в области защиты государственной тайны; • навыками определения надлежащих мер ответственности за нарушения законодательства в сфере защиты государственной тайны и информационной безопасности.
ПК-10. Способен принимать адекватные и соответствующие законодательству и ситуации управленческие решения в целях обеспечения национальной безопасности.	В результате освоения дисциплины студент должен: **Знать:** • основные угрозы безопасности при использовании информационных технологий; • меры ответственности за нарушение информационной безопасности; • назначение различных средств и систем защиты информации; • средства безопасности современных операционных систем; • способы защиты информации; • основы криптографических мер защиты информации; • организационные меры по защите информации. **Уметь:** • определять основные угрозы безопасности при использовании информационных технологий; • производить мониторинг безопасности информационных систем; • применить полученные знания в процессе дальнейшего обучения и своей профессиональной деятельности. **Практический опыт, владение:** • навыками выявления нарушений информационной безопасности; • навыками работы со встроенными средствами безопасности операционных систем и офисного программного обеспечения; • навыками безопасной работы в глобальных и локальных информационных сетях.

1.3. Содержание дисциплины

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины	Содержание
Р1	Введение	Определение понятия “информационная безопасность”. Информационная безопасность как отрасль. Роль и место информационной безопасности в профессиональной деятельности. Современное состояние и перспективы информационной безопасности. Государственное регулирование в сфере ИБ. Международные нормы и стандарты по ИБ.
Р2	Виды угроз ИБ	Классификация угроз информации и информационным технологиям. Субъекты ИБ. Угрозы доступности, целостности и конфиденциальности информации. Категории атак на информационные системы. Сценарий типовой атаки на информационную систему. Локальные атаки. Удаленные атаки. Атаки на поток данных. Атаки на пользователя (социальная инженерия).
Р3	Безопасность программного обеспечения	Средства защиты информации и обеспечения безопасности информационных технологий. Определение понятия «уязвимость программного обеспечения». Обзор методик тестирования и выявления уязвимостей. Организационные меры по обеспечению безопасности использования программного обеспечения. Меры защиты и подтверждения авторских прав на разрабатываемое программное обеспечение.
Р4	Встроенные средства безопасности операционных систем	Средства идентификации и аутентификации пользователей. Группы безопасности. Политика регистрации событий. Шифрование. Корпоративная безопасность. Службы сертификации. Встроенный Firewall. Политика ограничения используемых приложений. Средства электронной цифровой подписи. Защита от макровирусов. Централизованные средства управления. Компьютерные вирусы и антивирусные средства. Антивирусное программное обеспечение (АВПО). Обзор технологий и производителей АВПО. Практика применения АВПО. Эшелонированные системы антивирусной защиты. Атаки на АВПО.

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации.

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ» - проект ВС

Электронные ресурсы (издания)

1. Об информации, информационных технологиях и о защите информации. Федеральный закон № 149-ФЗ от 27.07.2006 (с изменениями и дополнениями) – Текст: электронный // КонсультантПлюс: [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/
2. Об электронной подписи. Федеральный закон № 63-ФЗ от 06.04.2011. – Текст: электронный // КонсультантПлюс: [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_112701/
3. О государственной тайне. Закон РФ № 5485-1 от 21.07.1993 (с изменениями и дополнениями) – Текст: электронный // КонсультантПлюс: [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_2481/
4. О коммерческой тайне. Федеральный закон № 98-ФЗ от 29.07.2004 (с изменениями и дополнениями). – Текст: электронный // КонсультантПлюс: [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_48699/
5. Закон РФ от 23.09.1992 N 3523-1 (ред. от 02.02.2006) "О правовой охране программ для электронных вычислительных машин и баз данных"– Текст: электронный // КонсультантПлюс: [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_1007/
6. Указ Президента РФ от 16.08.2004 N 1085 (ред. от 31.12.2015) "Вопросы Федеральной службы по техническому и экспортному контролю"– Текст: электронный // КонсультантПлюс: [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_14031/
7. Постановление Правительства РФ от 03.02.2012 N 79 (ред. от 15.06.2016) "О лицензировании деятельности по технической защите конфиденциальной информации" (вместе с "Положением о лицензировании деятельности по технической защите конфиденциальной информации") – Текст: электронный // КонсультантПлюс: [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_125798/
8. Постановление Правительства РФ от 03.03.2012 N 171 (ред. от 15.06.2016) "О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации" (вместе с "Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации") – Текст: электронный // КонсультантПлюс: [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_127010/
9. Меры защиты информации в государственных информационных системах. – Текст: электронный // Федеральная служба по техническому и экспортному контролю: [сайт]. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument
10. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год . – Текст: электронный // Федеральная служба по техническому и экспортному контролю: [сайт]. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god
11. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год .

– Текст: электронный // Федеральная служба по техническому и экспортному контролю: [сайт]. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god

12. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (части 1, 2, 3) . – Текст: электронный // Федеральная служба по техническому и экспортному контролю: [сайт]. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/381-rukovodyashchij-dokument
13. Руководящий документ. Защита от несанкционированного доступа к информации Часть 1. – Текст: электронный // Федеральная служба по техническому и экспортному контролю: [сайт]. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/382-rukovodyashchij-dokument-prikaz-predsedatelya-gostekhkomissii-rossii-ot-4-iyunya-1999-g-n-114
14. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации . – Текст: электронный // Федеральная служба по техническому и экспортному контролю: [сайт]. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g
15. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – Текст: электронный // Федеральная служба по техническому и экспортному контролю: [сайт]. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g
16. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. – Текст: электронный // Федеральная служба по техническому и экспортному контролю: [сайт]. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2
17. Защита от несанкционированного доступа к информации. Термины и определения. – Текст: электронный // Федеральная служба по техническому и экспортному контролю: [сайт]. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3
18. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. – Текст: электронный // Федеральная служба по техническому и экспортному контролю: [сайт]. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/387-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g4
19. Информационное сообщение об утверждении методических документов, содержащих профили защиты межсетевых экранов. – Текст: электронный // Федеральная служба по техническому и экспортному контролю: [сайт]. URL: http://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1184-informatsionnoe-soobshchenie-fstek-rossii-ot-12-sentyabrya-2016-g-n-240-24-4278
20. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 253 с. : ил. – Режим доступа: по подписке. –

URL: http://biblioclub.ru/index.php?page=book&id=276557 – Библиогр. в кн. – ISBN 978-5-4475-3946-7. – DOI 10.23681/276557. – Текст : электронный
21. Сагдеев, К.М. Физические основы защиты информации : учебное пособие / К.М. Сагдеев, В.И. Петренко, А.Ф. Чипига ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». – Ставрополь : СКФУ, 2015. – 394 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=458285 – Библиогр.: с. 387-388. – Текст : электронный.
22. Долозов, Н.Л. Программные средства защиты информации : конспект лекций / Н.Л. Долозов, Т.А. Гультяева ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2015. – 63 с. : схем., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=438307 – Библиогр. в кн. – ISBN 978-5-7782-2753-8. – Текст : электронный.
23. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 425 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=429070 – Библиогр. в кн. – Текст : электронный.
24. Аверченков, В.И. Служба защиты информации: организация и управление / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стер. – Москва : Флинта, 2016. – 186 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93356 – Библиогр. в кн. – ISBN 978-5-9765-1271-9. – Текст : электронный.
25. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. – 4-е изд., стер. – Москва : Флинта, 2016. – 224 с. – (Организация и технология защиты информации). – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93351 – Библиогр.: с. 192-193. – ISBN 978-5-9765-1274-0. – Текст : электронный.
26. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. – 3-е изд., стер. – Москва : Флинта, 2016. – 269 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93245 – Библиогр. в кн. – ISBN 978-5-9765-1256-6. – Текст : электронный.
27. Аудит информационной безопасности органов исполнительной власти : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский. – 4-е изд., стер. – Москва : Флинта, 2016. – 100 с. – (Организация и технология защиты информации). – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93259 – Библиогр.: с. 83-84. – ISBN 978-5-9765-1277-1. – Текст : электронный.

Печатные издания

Не предусмотрено

Профессиональные базы данных, информационно-справочные системы

1. Система ГАРАНТ: http://base.garant.ru/
2. Система Консультант: http://base.consultant.ru

Базы данных, информационно-справочные и поисковые системы

1. http://www.iso.org/ Международные стандарты безопасности ISO
2. http://fstec.ru/ Федеральная служба по техническому и экспортному контролю
3. www.consultant.ru – справочная система «Консультант-Плюс»;

4. www.garant.ru – справочная система «Гарант»;
5. http://window.edu.ru – единое окно доступа к образовательным ресурсам

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ» ПРОЕКТ ВС

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	Лекции;	Учебная аудитория для проведения занятий лекционного типа с мультимедийным оборудованием	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО

2	Практические занятия	Учебная аудитория для проведения лекционных занятий, практических занятий с мультимедийным оборудованием Компьютерный класс	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Пакет Statistica 13, договор № 43-12/963-2017/1 от 26.12.2017г., срок действия до 25.12.2020г. Project Expert 7.55 Tutorial (серверная версия - 20 одновременных подключений), договор № 43-12 199-2013 от 23.04.2013г., срок действия – бессрочный. IBM SPSS Statistics Standard Authorized User Licence svp_ed (лицензия: бессрочная академическая), договор 43-12 1726 2014 от 22.10.2014г. (8 лицензий), срок действия – бессрочный. VORTEX 8.0, договор № 264V от 24.03.2009г., срок действия – бессрочный. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО
3	Консультации	Учебная аудитория для проведения групповых и индивидуальных консультаций	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от

			05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО
4	Самостоятельная работа студентов	Учебная аудитория для проведения самостоятельной работы студентов	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-

			2017 от 25.08.2017г., срок действия – бессрочно. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО
5	Текущий и промежуточный контроль	Учебная аудитория для текущего контроля и промежуточной аттестации	Операционная система Microsoft Windows, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Офисный пакет Microsoft Office, подписка Desktop Education ALNG LicSAPk MVL B Faculty EES (Word, Excel, PowerPoint, Acsess, Visio, Outlook), договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. СУБД Microsoft SQL, подписка SQL Svr Standard Core ALNG LicSAPk MVL 2Lic CoreLic EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Microsoft Project, подписка Project Professional ALNG LicSAPk MVL w1Project Server CAL EES, договор № 43-12/1864-2018 от 05.12.2018г., срок действия до 31.01.2020г. Система распознавания текста ABBYY FineReader 14, договор № 43-12/1047-2017 от 25.08.2017г., срок действия – бессрочно. Браузер Google Chrome – свободное ПО Браузер Mozilla Firefox – свободное ПО