Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Проректор по учебной работе
к.э.н., доцент Изместьев А.А

_____

17.06.2019г.

Рабочая программа дисциплины
Б1.Б.5. Основы информационной безопасности в профессиональной деятельности

Направление подготовки (специальность): 45.05.01 Перевод и переводоведение
Специализация: Лингвистическое обеспечение межгосударственных отношений
Квалификация выпускника: лингвист-переводчик
Форма обучения: очная

Курс	2
Семестр	22
Лекции (час)	36
Практические (сем, лаб.) занятия (час)	0
Самостоятельная работа, включая подготовку к экзаменам и зачетам (час)	108
Курсовая работа (час)	
Всего часов	144
Зачет (семестр)	
Экзамен (семестр)	22

Иркутск 2019

Программа составлена в соответствии с ФГОС ВО по направлению 45.05.01 Перевод и переводоведение.

Автор М.М. Бусько

Рабочая программа обсуждена и утверждена на заседании кафедры математических методов и цифровых технологий

Заведующий кафедрой А.В. Родионов

Дата актуализации рабочей программы: 30.06.2020

1. Цели изучения дисциплины

Цель курса — изучение комплекса проблем информационной безопасности в профессиональной деятельности переводчика; построения, функционирования и совершенствования правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации; изучение понятий и видов защищаемой информации по законодательству РФ, системы защиты государственной тайны.

Задачи курса:

- овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности;
- освоение системных комплексных методов защиты информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения;
- ознакомление с современными законодательными и нормативно-правовыми проблемами обеспечения информационной безопасности;
- приобретение теоретических и практических навыков по основам использования современных методов правовой защиты государственной, коммерческой, служебной, профессиональной и личной тайны, персональных данных в компьютерных системах;
- овладение знаниями и умениями соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;
- формирование способности понимать сущность и значение информации в развитии современного информационного общества, соблюдать основные требования информационной безопасности
- освоение практических навыков и способностей осуществления мероприятий по обеспечению правовой защиты информации.

Изучаемые вопросы рассматриваются в широком диапазоне современных проблем и затрагивают предметные сферы защиты как документированной информации (на бумажных и технических носителях), циркулирующей в традиционном или электронном документообороте, находящейся в компьютерных системах, так и недокументированной информации, распространяемой персоналом в процессе управленческой (деловой) или производственной деятельности.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Компетенции обучающегося, формируемые в результате освоения дисциплины

Код компетенции по ФГОС ВО	Компетенция
ОПК-2	способность соблюдать в профессиональной деятельности требования правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, обеспечивать соблюдение режима секретности

Структура компетенции

Компетенция	Формируемые ЗУНы
ОПК-2 способность соблюдать в профессиональной деятельности требования	З. Знать требование правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа

правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, обеспечивать соблюдение режима секретности	У. Уметь соблюдать в профессиональной деятельности основные требования информационной безопасности, в том числе защиты государственной, служебной и личной тайны Н. Владеть навыками применения требований правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, соблюдения режима секретности

3. Место дисциплины (модуля) в структуре образовательной программы

Принадлежность дисциплины - БЛОК 1 ДИСЦИПЛИНЫ (МОДУЛИ): Базовая часть.

Предшествующие дисциплины (освоение которых необходимо для успешного освоения данной): "Правоведение"

4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 4 зач. ед.,144 часов.

Вид учебной работы	Количество часов
Контактная(аудиторная) работа	
Лекции	36
Практические (сем, лаб.) занятия	0
Самостоятельная работа, включая подготовку к экзаменам и зачетам	108
Всего часов	144

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1. Содержание разделов дисциплины

№ п/п	Раздел и тема дисциплины	Семе-стр	Лек-ции	Семинар Лаборат. Практич.	Само-стоят. раб.	В интера-ктивной форме	Формы текущего контроля успеваемости
1	Основы информационной безопасности. Правовая защита информации	22	6		18		Тест
2	Организационная защита информации	22	6		18		Тест
3	Защита информации в компьютерных информационных системах	22	6		18		Тест
4	Криптографические методы защиты информации	22	6		18		Тест

№ п/п	Раздел и тема дисциплины	Семе-стр	Лек-ции	Семинар Лаборат. Практич.	Само-стоят. раб.	В интера-ктивной форме	Формы текущего контроля успеваемости
5	Защита информации от разрушающих программных воздействий	22	6		18		Тест
5	Информационная безопасность в профессиональной сфере	22	6		18		Тест
	ИТОГО		36		108		

5.2. Лекционные занятия, их содержание

№ п/п	Наименование разделов и тем	Содержание
01	Лекция 1	Понятие информационной безопасности. Актуальность информационной безопасности. Принципы обеспечения информационной безопасности. Структура информационной безопасности. Структура системы защиты информации РФ.
02	Лекция 2	Угрозы безопасности в информационной сфере. Структура нормативной базы Российской Федерации по вопросам информационной безопасности. Правовая защита интересов личности, общества и государства от информационных угроз.
03	Лекция 3	Классификация информации по видам тайны и степеням конфиденциальности. Защита государственной тайны. Защита коммерческой тайны. Защита персональных данных.
04	Лекция 4	Общая характеристика организационных методов защиты информации. Виды каналов утечки информации на предприятии. Зоны ответственности. Локальные нормативные акты в области информационной безопасности.
05	Лекция 5	Организация службы безопасности предприятия. Организация внутриобъектового режима на предприятия. Организация охраны объектов предприятия. Организация инженерно-технической безопасности. Средства выявления каналов утечки информации. Методы и способы защиты информации от утечки по техническим каналам.
06	Лекция 6	Разглашение защищаемой информации. Способы пресечения разглашения защищаемой информации. Противодействие несанкционированному доступу к информации. Грифы ограничения доступа к документам. Организация конфиденциального документооборота.
07	Лекция 7	Анализ угроз информационной безопасности компьютерных систем. Технологии защиты информации в компьютерных системах.
08	Лекция 8	Идентификация, аутентификация и управление доступом. Обеспечение безопасности операционных систем. Технологии межсетевого экранирования. Технологии виртуальных защищенных сетей (VPN). Анализ защищенности и обнаружение атак. Технологии резервного копирования и восстановления данных.

№ п/п	Наименование разделов и тем	Содержание
09	Лекция 9	Условия существования вредоносных программ. Классификация вредоносных программ. Основы работы антивирусных программ. Защита компьютерных систем от воздействия вредоносных программ. Защита от СПАМА
10	Лекция 10	Шифрование. Классификация методов криптографического закрытия информации. Симметричные криптосистемы. Криптосистемы с открытым ключом. Квантовая криптография.
11	Лекция 11	Стеганография. Контроль целостности. Хэш-функции. MAC-коды. Электронная подпись. Открытый и закрытый ключи в электронной цифровой подписи.
12	Лекция 12	Методики ассиметричного шифрования, используемые при формировании ЭП. Закон об электронной цифровой подписи. Программные средства и технологии формирования электронной цифровой подписи.
13	Лекция 13	Классификация средств исследования программ. Методы защиты программ от исследования.
14	Лекция 14	Условия существования вредоносных программ. Общая характеристика и классификация компьютерных вирусов. Основы работы антивирусных программ.
15	Лекция 15	Общая характеристика средств нейтрализации компьютерных вирусов. Классификация методов защиты от компьютерных вирусов. Защита от СПАМА.
16	Лекция 16	Информационное оружие. Компьютерные вирусы. Деблокеры. Информационные войны. Компьютерные преступления (киберпреступность). Киберпреследование. Способы защиты от киберпреследования. Кадровое и ресурсное обеспечение защиты информации. Подбор и подготовка кадров.
17	Лекция 17	Проверка персонала на благонадежность. Особенности увольнения сотрудников, владеющих конфиденциальной информацией. Переговорный процесс и обеспечение информационной безопасности. Переговорный процесс как способ разрешения конфликтных ситуаций. Виды переговоров. Стратегии переговоров. Роль переводчика в переговорном процессе. Защита информации при работе в сети Интернет.
18	Лекция 18	Признаки незаконного проникновения в компьютерную систему. Дальнейшие действия в случае обнаружения незаконного проникновения в компьютерную систему. Ответственность, за правонарушения в области информационной безопасности.

5.3. Семинарские, практические, лабораторные занятия, их содержание

6. Фонд оценочных средств для проведения промежуточной аттестации по дисциплине (полный текст приведен в приложении к рабочей программе)

6.1. Текущий контроль

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
1	1. Основы информационной безопасности. Правовая защита информации	ОПК-2	З.Знать требование правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа У.Уметь соблюдать в профессиональной деятельности основные требования информационной безопасности, в том числе защиты государственной, служебной и личной тайны Н.Владеть навыками применения требований правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, соблюдения режима секретности	Тест	18-20 — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки. 14-17 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков. 8-13 баллов — общие, но не структурированные знания; не систематически осуществляе-мые умения; не систематически применяемые навыки. 8 и менее баллов — студент обнаружил несостоятельность ответов (20)
2	2. Организационная защита информации	ОПК-2	З.Знать требование правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа У.Уметь соблюдать в	Тест	18-20 — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки. 14-17 баллов — сформированные,

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
			профессиональной деятельности основные требования информационной безопасности, в том числе защиты государственной, служебной и личной тайны Н.Владеть навыками применения требований правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, соблюдения режима секретности		но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков. 8-13 баллов — общие, но не структурированные знания; не систематически осуществляе-мые умения; не систематически применяемые навыки. 8 и менее баллов — студент обнаружил несостоятельность ответов (20)
3	3. Защита информации в компьютерных информационных системах	ОПК-2	З.Знать требование правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа У.Уметь соблюдать в профессиональной деятельности основные требования информационной безопасности, в том числе защиты государственной, служебной и личной тайны Н.Владеть навыками применения	Тест	18-20 — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки. 14-17 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
			требований правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, соблюдения режима секретности		отдельные пробелы применение навыков. 8-13 баллов — общие, но не структурированные знания; не систематически осуществляе-мые умения; не систематически применяемые навыки. 8 и менее баллов — студент обнаружил несостоятельность ответов (20)
4	4. Криптографические методы защиты информации	ОПК-2	З.Знать требование правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа У.Уметь соблюдать в профессиональной деятельности основные требования информационной безопасности, в том числе защиты государственной, служебной и личной тайны Н.Владеть навыками применения требований правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, соблюдения режима секретности	Тест	18-20 — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки. 14-17 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков. 8-13 баллов — общие, но не структурированные знания; не систематически осуществляе-мые умения; не

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
					систематически применяемые навыки. 8 и менее баллов — студент обнаружил несостоятельность ответов (20)
5	5. Защита информации от разрушающих программных воздействий	ОПК-2	З.Знать требование правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа У.Уметь соблюдать в профессиональной деятельности основные требования информационной безопасности, в том числе защиты государственной, служебной и личной тайны Н.Владеть навыками применения требований правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, соблюдения режима секретности	Тест	9-10 баллов — сформированные систематические знания; на высоком уровне осуществляе-мые умения, успешно применяемые навыки; 7-8 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 5-6 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не си-стематически применяемые навыки; 4 и менее баллов — студент обнаружил несостоятель-ность ответов (10)
6		ОПК-2	З.Знать требование правовых актов в	Тест	9-10 баллов — сформированные

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	(ЗУНы: (З.1…З.n, У.1…У.n, Н.1…Н.n)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
			области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа У.Уметь соблюдать в профессиональной деятельности основные требования информационной безопасности, в том числе защиты государственной, служебной и личной тайны Н.Владеть навыками применения требований правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, соблюдения режима секретности		систематические знания; на высоком уровне осуществляе-мые умения, успешно применяемые навыки; 7-8 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 5-6 баллов — общие, но не структурированн ые знания; не систематически осуществляемые умения; не си-стематически применяемые навыки; 4 и менее баллов — студент обнаружил несостоятель-ность ответов (10)
				Итого	**100**

6.2. Промежуточный контроль (зачет, экзамен)

Рабочим учебным планом предусмотрен Экзамен в семестре 22.

ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ:

1-й вопрос билета (30 баллов), вид вопроса: Тест/проверка знаний. Критерий: Каждый вопрос теста 2 балла..

Компетенция: ОПК-2 способность соблюдать в профессиональной деятельности требования правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, обеспечивать соблюдение режима секретности

Знание: Знать требование правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа

1. Актуальность информационной безопасности.
2. Анализ защищенности и обнаружение атак.
3. Анализ защищенности информационной системы.
4. Анализ угроз информационной безопасности компьютерных систем.
5. Грифы ограничения доступа к документам.
6. Защита государственной тайны.
7. Защита коммерческой тайны.
8. Защита компьютерных систем от воздействия вредоносных программ.
9. Защита от СПАМА.
10. Защита персональных данных.
11. Идентификация, аутентификация и управление доступом.
12. Инженерно-техническая защита информации.
13. Квантовая криптография.
14. Классификация вредоносных программ.
15. Классификация информации по видам тайны и степеням конфиденциальности.
16. Классификация методов криптографического закрытия информации.
17. Комплексный подход к защите информации.
18. Криптосистемы с открытым ключом.
19. Лицензирование, сертификация и аттестация в сфере защиты информации.
20. Локальные нормативные акты в области информационной безопасности.
21. Методы и способы защиты информации от утечки по техническим каналам.
22. Обеспечение безопасности операционных систем.
23. Организационная защита информации. Зоны ответственности.
24. Организация конфиденциального документооборота.
25. Организация службы безопасности предприятия.
26. Основы работы антивирусных программ.
27. Ответственность, за правонарушения в области информационной безопасности.
28. Понятие информационной безопасности.
29. Правовая защита интересов личности, общества и государства от информационных угроз.
30. Практические правила управления информационной безопасностью.
31. Принципы обеспечения информационной безопасности.
32. Симметричные криптосистемы.
33. Средства выявления каналов утечки информации.
34. Стандарты и спецификации в области информационной безопасности.
35. Стеганография.
36. Структура информационной безопасности.
37. Структура нормативной базы Российской Федерации по вопросам информационной безопасности.
38. Структура системы защиты информации РФ.
39. Технические каналы утечки информации.
40. Технологии виртуальных защищенных сетей (VPN).
41. Технологии защиты информации в компьютерных системах.

42. Технологии межсетевого экранирования.
43. Технологии резервного копирования и восстановления данных.
44. Угрозы безопасности в информационной сфере.
45. Управление информационной безопасностью.
46. Условия существования вредоносных программ.
47. Физическая укрепленность объекта информатизации.
48. Электронная подпись.

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ УМЕНИЙ:

2-й вопрос билета (35 баллов), вид вопроса: Задание на умение. Критерий: 32-35 баллов — заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание учебного материала, самостоятельно ответивший на вопросы, ответ отличается богатством и точностью использованных терминов, материал излагается последовательно и логично; 25-32 балла — заслуживает студент, обнаруживший полное знание учебного материала, не допускающий в ответе существенных неточностей, самостоятельно ответивший на вопросы; 14-25 баллов — заслуживает студент, обнаруживший знание основного учебного материала в объёме, необходимом для дальнейшей учебы, однако допустивший некоторые погрешности при ответе на вопросы; 13 и менее — выставляется студенту, обнаружившему пробелы в знаниях или отсутствие знаний по значительной части основного учебного материала, допустившему принципиальные ошибки при ответе на вопросы.

Компетенция: ОПК-2 способность соблюдать в профессиональной деятельности требования правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, обеспечивать соблюдение режима секретности
Умение: Уметь соблюдать в профессиональной деятельности основные требования информационной безопасности, в том числе защиты государственной, служебной и личной тайны
Задача № 1. Определите к какому типу по ограничению доступа относится информация, представленная в вашем варианте задания и объясните какие нормативно-правовые документы устанавливают этот статус.
Задача № 2. Установите правовой статус информации со ссылкой на нормативные документы и определите какие свойства информационной безопасности следует поддерживать.

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ НАВЫКОВ:

3-й вопрос билета (35 баллов), вид вопроса: Задание на навыки. Критерий: 32-35 баллов — заслуживает студент, выполнивший задание в соответствии с заявленной инструкцией или технологией, полностью и правильно; сделаны глубокие и детальные выводы с опорой на источники; имеются ссылки на нормативные документы, не нарушены сроки выполнения задания; 25-32 баллов — заслуживает студент, за правильное выполнение задания в соответствии с инструкцией или технологией с учетом 2-3 несущественных ошибок; выводы сформулированы корректно со ссылкой на источники и нормативные документы; сроки выполнения задания не нарушены; 14-25 — заслуживает студент за выполнение задания правильно не менее чем на половину или если допущена существенная ошибка; выводы сформулированы поверхностно, некорректно; отсутствуют ссылки на источники; сроки выполнения задания не нарушены; 13 и менее — выставляется студенту, если при выполнении задания допущены две (и более) существенные ошибки или задание не выполнено вообще; выводы сформулированы с грубыми ошибками или отсутствуют вообще; задание выполнено с нарушением сроков.

Компетенция: ОПК-2 способность соблюдать в профессиональной деятельности требования правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, обеспечивать соблюдение режима секретности

Навык: Владеть навыками применения требований правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, соблюдения режима секретности

Задание № 1. В соответствии с методическими документами ФСТЭК определить параметры защищенности информации для ситуаций, представленных в варианте задания

Задание № 2. Определить необходимые меры защиты, регламентированные нормативно-методическими документами произвести выбор необходимых средств защиты для ситуаций, описанных в варианте задания.

ОБРАЗЕЦ БИЛЕТА

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «БГУ»)

Направление - 45.05.01 Перевод и переводоведение
Профиль - Лингвистическое обеспечение межгосударственных отношений
Кафедра математических методов и цифровых технологий
Дисциплина - Основы информационной безопасности в профессиональной деятельности

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Тест (30 баллов).
2. Установите правовой статус информации со ссылкой на нормативные документы и определите какие свойства информационной безопасности следует поддерживать. (35 баллов).
3. В соответствии с методическими документами ФСТЭК определить параметры защищенности информации для ситуаций, представленных в варианте задания (35 баллов).

Составитель _____ М.М. Бусько

Заведующий кафедрой _____ А.В. Родионов

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

а) основная литература:

1. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. допущено УМО по образованию в обл. прикладной информатики. учеб. пособие. 3-е изд., перераб. и доп./ Е. К. Баранова, А. В. Бабаш.- М.: ИНФРА-М, 2016.-321 с.
2. Гришина Н. В. Информационная безопасность предприятия. учеб. пособие для вузов. рек. УМО вузов РФ по образованию в обл. историко-архивоведения. 2-е изд., доп./ Н. В. Гришина.- М.: ИНФРА-М, 2017.-238 с.

3.
4. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ В.А. Галатенко— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 с.— Режим доступа: http://www.iprbookshop.ru/52209.html.— ЭБС «IPRbooks» [08.09.2017]
5. Горина Е.В. Коммуникативные технологии манипуляции в СМИ и вопросы информационной безопасности [Электронный ресурс] : учебно-методическое пособие / Е.В. Горина. — Электрон. текстовые данные. — Екатеринбург: Уральский федеральный университет, 2016. — 68 с. — 978-5-7996-1807-0. — Режим доступа: http://www.iprbookshop.ru/66538.html
6. Коваленко Ю.И. Методика защиты информации в организациях [Электронный ресурс]: монография/ Ю.И. Коваленко, Г.И. Москвитин, М.М. Тараскин— Электрон. текстовые данные.— М.: Русайнс, 2016.— 162 с.— Режим доступа: http://www.iprbookshop.ru/61625.html.— ЭБС «IPRbooks» [08.09.2017]

б) дополнительная литература:

1. Астахова А. В. Информационные системы в экономике и защита информации на предприятиях-участниках ВЭД. учеб. пособие для вузов/ А. В. Астахова.- СПб.: Троицкий мост, 2014.-214 с.
2. Гугуева Т. А. Конфиденциальное делопроизводство. учеб. пособие для вузов. 2-е изд., перераб. и доп./ Т. А. Гугуева.- М.: ИНФРА-М, 2017.-198 с.
3.
4. Банк данных угроз безопасности информации. Федеральная служба по техническому и экспортному контролю. Государственный научно-исследовательский испытательный институт проблем технической защиты информации. http://bdu.fstec.ru/ (30.08.2017)
5. Горбенко А.О. Основы информационной безопасности (введение в профессию) [Электронный ресурс] : учебное пособие / А.О. Горбенко. — Электрон. текстовые данные. — СПб. : Интермедия, 2017. — 335 с. — 978-5-4383-0136-3. — Режим доступа: http://www.iprbookshop.ru/66797.html
6. Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00. http://fstec.ru/component/attachments/download/489
7. Перечень средств защиты информации, сертифицированных ФСБ России. http://clsz.fsb.ru/files/download/svedenia_po_sertifikatam_(010717).doc
8. Рагозин Ю.Н. Инженерно-техническая защита информации [Электронный ресурс] : учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности / Ю.Н. Рагозин. — Электрон. текстовые данные. — СПб. : Интермедия, 2018. — 168 с. — 978-5-4383-0161-5. — Режим доступа: http://www.iprbookshop.ru/73641.html
9. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 424 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52161.html
10. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 с. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля), включая профессиональные базы данных и информационно-справочные системы

Для освоения дисциплины обучающемуся необходимы следующие ресурсы информационно-телекоммуникационной сети «Интернет»:

– Сайт Байкальского государственного университета, адрес доступа: http://bgu.ru/, доступ круглосуточный неограниченный из любой точки Интернет
– ИВИС - Универсальные базы данных, адрес доступа: http://www.dlib.eastview.ru/. доступ круглосуточный неограниченный из любой точки Интернет при условии регистрации в БГУ
– КиберЛенинка, адрес доступа: http://cyberleninka.ru. доступ круглосуточный, неограниченный для всех пользователей, бесплатное чтение и скачивание всех научных публикаций, в том числе пакет «Юридические науки», коллекция из 7 журналов по правоведению
– Научная электронная библиотека eLIBRARY.RU, адрес доступа: http://elibrary.ru/. доступ к российским журналам, находящимся полностью или частично в открытом доступе при условии регистрации
– Национальный цифровой ресурс «Руконт», адрес доступа: http://www.rucont.ru. доступ неограниченный
– Федеральная служба безопасности Российской Федерации, адрес доступа: http://fsb.ru. доступ неограниченный
– Федеральная служба по техническому и экспортному контролю, адрес доступа: http://fstec.ru. доступ неограниченный
– Федеральный образовательный портал «Экономика, Социология, Менеджмент», адрес доступа: http://www.ecsocman.edu.ru. доступ неограниченный
– ЭБС BOOK.ru - электронно-библиотечная система от правообладателя, адрес доступа: http://www.book.ru/. доступ неограниченный
– Электронная библиотека Издательского дома "Гребенников", адрес доступа: http://www.grebennikon.ru/. доступ с компьютеров сети БГУ (по IP-адресам)
– Электронно-библиотечная система IPRbooks, адрес доступа: https://www.iprbookshop.ru. доступ неограниченный

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Изучать дисциплину рекомендуется в соответствии с той последовательностью, которая обозначена в ее содержании. Для успешного освоения курса обучающиеся должны иметь первоначальные знания в области информационных технологий.

На лекциях преподаватель озвучивает тему, знакомит с перечнем литературы по теме, обосновывает место и роль этой темы в данной дисциплине, раскрывает ее практическое значение. В ходе лекций студенту необходимо вести конспект, фиксируя основные понятия и проблемные вопросы.

Практические (семинарские) занятия по своему содержанию связаны с тематикой лекционных занятий. Начинать подготовку к занятию целесообразно с конспекта лекций. Задание на практическое (семинарское) занятие сообщается обучающимся до его проведения. На семинаре преподаватель организует обсуждение этой темы, выступая в качестве организатора, консультанта и эксперта учебно-познавательной деятельности обучающегося.

Изучение дисциплины (модуля) включает самостоятельную работу обучающегося.

Основными видами самостоятельной работы студентов с участием преподавателей являются:

• текущие консультации;

• коллоквиум как форма контроля освоения теоретического содержания дисциплин: (в часы консультаций, предусмотренные учебным планом);

• прием и разбор домашних заданий (в часы практических занятий);

• прием и защита лабораторных работ (во время проведения занятий);

• выполнение курсовых работ в рамках дисциплин (руководство, консультирование и защита курсовых работ в часы, предусмотренные учебным планом) и др.

Основными видами самостоятельной работы студентов без участия преподавателей являются:

• формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

• самостоятельное изучение отдельных тем или вопросов по учебникам или учебным пособиям;

• написание рефератов, докладов;

• подготовка к семинарам и лабораторным работам;

• выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и др.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

В учебном процессе используется следующее программное обеспечение:
– Гарант платформа F1 7.08.0.163 - информационная справочная система,
– КонсультантПлюс: Версия Проф - информационная справочная система,
– MS Office,

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю):

В учебном процессе используется следующее оборудование:
– Помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду вуза,
– Учебные аудитории для проведения: занятий лекционного типа, занятий семинарского типа, практических занятий, выполнения курсовых работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения,
– Компьютерный класс,
– Наборы демонстрационного оборудования и учебно-наглядных пособий