Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Проректор по учебной работе
к.э.н., доцент Волченко Л.Ю

_____

25.05.2018г.

Рабочая программа дисциплины
Б1.ДВ.1. Защита персональных данных

Направление подготовки (специальность): 37.05.02 Психология служебной деятельности
Специализация: Морально-психологическое обеспечение служебной деятельности
Квалификация выпускника: психолог
Форма обучения: очная, очно-заочная

	Очная ФО	Очно-заочная ФО
Курс	3	3
Семестр	31	32
Лекции (час)	14	0
Практические (сем, лаб.) занятия (час)	28	18
Самостоятельная работа, включая подготовку к экзаменам и зачетам (час)	66	90
Курсовая работа (час)		
Всего часов	108	108
Зачет (семестр)	31	32
Экзамен (семестр)		

Иркутск 2018

Программа составлена в соответствии с ФГОС ВО по направлению 37.05.02 Психология служебной деятельности.

Автор М.М. Бусько

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

Заведующий кафедрой С.С. Ованесян

Дата актуализации рабочей программы: 28.06.2019
Дата актуализации рабочей программы: 30.06.2020

1. Цели изучения дисциплины

Целью освоения дисциплины защита персональных данных является формирование правовой грамотности, понятия персональных данных, изучение особенности защиты персональных данных, принципов моделирования угроз безопасности ПДн, принципов построения системы защиты информации ограниченного доступа.

Задачи дисциплины:

- ознакомление с нормативно-правовым обеспечением безопасности ПДн, методиками определения уровня защищенности информационных систем обработки персональных данных (ИСПДн);
- рассмотрение различных классов современных технических средств защиты информации, изучение их принципов действия, характеристик и функциональных возможностей;
- получение теоретических знаний и практических навыков по выявлению угроз безопасности ПДн при их обработке в ИСПДн, по выявлению каналов утечки конфиденциальной информации, построению модели нарушителя информационной безопасности ПДн, использованию программно-аппаратных комплексов для оценки защищенности объектов информатизации от утечки информации по техническим каналам.

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
ПК-29	способность соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности
ПСК-2	способность обеспечивать личную безопасность и безопасность граждан в процессе выполнения служебных задач

Структура компетенции

Компетенция	Формируемые ЗУНы
ПК-29 способность соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	З. знать требования правовых актов в области защиты государственной тайны и информационной безопасности У. уметь соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, уметь обеспечивать соблюдение режима секретности Н. владеть навыками соблюдения в профессиональной деятельности требований правовых актов в области защиты государственной тайны и информационной безопасности
ПСК-2 способность обеспечивать личную безопасность и безопасность граждан в процессе выполнения служебных задач	З. знать основные требования к обеспечению личной безопасности и безопасность граждан в процессе выполнения служебных задач У. уметь обеспечивать личную безопасность и безопасность граждан в процессе выполнения служебных задач

	Н. владеть навыками обеспечения личной безопасности и безопасности граждан в процессе выполнения служебных задач

3. Место дисциплины (модуля) в структуре образовательной программы

Принадлежность дисциплины - БЛОК 1 ДИСЦИПЛИНЫ (МОДУЛИ): Дисциплина по выбору.

Предшествующие дисциплины (освоение которых необходимо для успешного освоения данной): "Информатика и информационные технологии в психологии", "Правоведение", "Социология"

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 3 зач. ед.,108 часов.

Вид учебной работы	Количество часов (очная ФО)	Количество часов (очно-заочная ФО)
Контактная(аудиторная) работа		
Лекции	14	0
Практические (сем, лаб.) занятия	28	18
Самостоятельная работа, включая подготовку к экзаменам и зачетам	66	90
Всего часов	108	108

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

Очно-заочная форма обучения

№ п/п	Раздел и тема дисциплины	Семестр	Лекции	Семинар Лаборат. Практич.	Самостоят. раб.	В интерактивной форме	Формы текущего контроля успеваемости
1	Реализация конституционных прав граждан на неприкосновенность частной жизни	32	0	2	10		Практическая работа №1
2	Принципы обработки персональных данных	32	0	2	10		Практическая работа №2
3	Практические вопросы реализации Федерального закона «О персональных данных» от 27 июля 2006 года № 152-ФЗ	32	0	2	12		Практическая работа №3
4	Нормативно-	32	0	2	12		Практическая

№ п/п	Раздел и тема дисциплины	Семе-стр	Лек-ции	Семинар Лаборат. Практич.	Само-стоят. раб.	В интера-ктивной форме	Формы текущего контроля успеваемости
	методическое обеспечение безопасности информационных систем персональных данных						работа №4
5	Специфика работы с персональными данными в организации (учреждении, предприятии)	32	0	4	12		Практическая работа №5
6	Методы защиты информационных систем персональных данных	32	0	2	12		Практическая работа №6
7	Организация и обеспечение режимов защиты персональных данных	32	0	2	12		Практическая работа №7
8	Оценка эффективности систем защиты информационных систем персональных данных	32	0	2	10		Практическая работа №8
	ИТОГО			18	90		

Очная форма обучения

№ 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	Тема 1.Реализация конституционных прав граждан на неприкосновенность частной жизни	31	2	4	8		Практическая работа №1
2	Тема 2. Принципы обработки персональных данных	31	2	4	10		Практическая работа №2
3	Тема 3. Практические вопросы реализации Федерального закона «О персональных данных» от 27 июля 2006 года № 152-ФЗ	31	2	4	10		Практическая работа №3
4	Тема 4. Нормативно-методическое обеспечение безопасности информационных	31	2	4	10		Практическая работа №4

№ п/п	Раздел и тема дисциплины	Семе-стр	Лек-ции	Семинар Лаборат. Практич.	Само-стоят. раб.	В интера-ктивной форме	Формы текущего контроля успеваемости
	систем персональных данных						
5	Тема 5. Специфика работы с персональными данными в организации (учреждении, предприятии)	31	2	4	10		Практическая работа №5
6	Тема 6. Методы защиты информационных систем персональных данных	31	2	4	10		Практическая работа №6
7	Тема 7. Организация и обеспечение режимов защиты персональных данных	31	2	4	8		Практическая работа №7
	ИТОГО		14	28	66		

5.2. Лекционные занятия, их содержание

№ п/п	Наименование разделов и тем	Содержание
1	Реализация конституционных прав граждан на неприкосновенность частной жизни	Понятие права на неприкосновенность частной жизни, его определение. Характеристики информации о частной жизни гражданина. Информация о частной жизни граждан и персональные данные. Определение связи с понятием «персональные данные». Основы законодательства в области персональных данных. Определение понятия «персональные данные». Персональные данные в Федеральном законе и Трудовом кодексе Российской Федерации. Содержание категории «персональные данные». Обработка персональных данных: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (передача), обезличивание, блокирование, уничтожение
2	Принципы обработки персональных данных	Основные положения закона «О персональных данных» от 27 июля 2006 года № 152-ФЗ. Сфера регулирования. Категории персональных данных. Биометрические персональные данные, специальные категории персональных данных. Обезличенные персональные данные. Основные принципы обработки персональных данных. Условия обработки персональных данных. Требования к операторам персональных данных. Ответственность операторов персональных данных. Права субъектов персональных данных и их соблюдение при обработке
3	Практические вопросы реализации Федерального закона «О персональных	Понятие персональных данных, и их интерпретация. Категорирование информации, содержащей персональные данные. Практические вопросы исполнения операторами персональных данных своих обязанностей. Вопрос автономии

№ п/п	Наименование разделов и тем	Содержание
	данных» от 27 июля 2006 года № 152-ФЗ	операторов в выборе мер защиты персональных данных. Обработка персональных данных третьим лицом в интересах оператора. Обязанности оператора персональных данных в ходе сбора и обработки персональных данных, ответы на запросы субъектов. Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных. Ответственность за нарушение требований по обращению с персональными данными
4	Нормативно-методическое обеспечение безопасности информационных систем персональных данных	Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Порядок проведения классификации информационных систем персональных данных. Руководящие документы ФСТЭК и ФСБ России по защите персональных данных. Нормативно-методическое обеспечение безопасности информационных систем персональных данных в органах власти, учреждениях (предприятиях)
5	Специфика работы с персональными данными в организации (учреждении, предприятии)	Основные локальные нормативные акты для организации работы с персональными данными. Сферы их регулирования и структура. Перечень необходимой информации для организации выполнения требований законодательства. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Модель злоумышленника информационных систем персональных данных. Разработка частных моделей угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования. Локальные нормативные акты организации, составляемые с учетом требований Роскомнадзора в области защиты персональных данных
6	Методы защиты информационных систем персональных данных	Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Мероприятия по защите сведений конфиденциального характера, основные внутренние нормативные документы, меры по охране конфиденциальности; формирование перечня персональных данных. Ограничение доступа к персональным данным, учет лиц, допущенных к персональным данным, определение порядка обращения с такими сведениями, контроля над его соблюдением, организация доступа к персональным данным, внутренние нормативные документы по охране конфиденциальности сведений, их содержание, порядок разработки и ввода в действие, контроль над соблюдением режима конфиденциальности
7	Организация и обеспечение режимов защиты персональных	Организация защиты персональных данных обрабатываемых автоматизированным способом. Требования, методы и средства. Порядок создания системы защиты персональных данных от несанкционированных воздействий по техническим

№ п/п	Наименование разделов и тем	Содержание
	данных	каналам. Организация защиты персональных данных обрабатываемых неавтоматизированным способом. Требования, методы и средства. Стратегия защиты персональных данных. Организационные и технические мероприятия, направленные на минимизацию ущерба от возможной реализации угроз безопасности персональных данных. Защита персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий. Лицензирование деятельности по технической защите конфиденциальной информации при защите персональных данных. Основные требования для получения лицензии

5.3. Семинарские, практические, лабораторные занятия, их содержание

№ раздела и темы	Содержание и формы проведения
1	Семинар 1. Выполнение практической работы №1
1	Семинар 2. Защита отчета по выполненной работе №1
2	Семинар 3. Выполнение практической работы №2
2	Семинар 4. Защита отчета по выполненной работе №2
3	Семинар 5. Выполнение практической работы №3
3	Семинар 6. Защита отчета по выполненной работе №3
4	Семинар 7. Выполнение практической работы №4
4	Семинар 8. Защита отчета по выполненной работе №4
5	Семинар 9. Выполнение практической работы №5
5	Семинар 10. Защита отчета по выполненной работе №5
6	Семинар 11. Выполнение практической работы №6
6	Семинар 12. Защита отчета по выполненной работе №6
7	Семинар 13. Выполнение практической работы №7
7	Семинар 14. Защита отчета по выполненной работе №7

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. Тема 1.Реализация конституционных	ПК-29	З.знать требования правовых актов в области защиты	Практическая работа №1	9-10 баллов — сформированные систематические

№ 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)
	прав граждан на неприкосновенность частной жизни		государственной тайны и информационной безопасности У.уметь соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, уметь обеспечивать соблюдение режима секретности Н.владеть навыками соблюдения в профессиональной деятельности требований правовых актов в области защиты государственной тайны и информационной безопасности		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)
2	2. Тема 2. Принципы обработки персональных данных	ПСК-2	З.знать основные требования к обеспечению личной безопасности и безопасность граждан в процессе выполнения служебных задач У.уметь обеспечивать личную безопасность и безопасность граждан в процессе выполнения	Практическая работа №2	14-15 баллов — сформированные систематические знания; на высоком уровне осуществляе-мые умения, успешно применяемые навыки; 11-13 баллов — сформированные, но содержа-щие отдельные

№ 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)
			служебных задач Н.владеть навыками обеспечения личной безопасности и безопасности граждан в процессе выполнения служебных задач		пробелы знания; в целом успешные, но содержащие отдельные пробелы уме-ния; в целом успешное, но содержащее отдельные пробелы применение навыков; 7-10 баллов — общие, но не структурированн ые знания; не систематически осуществляемые умения; не систематически применяемые навыки; 6 и менее баллов — студент обнаружил несостоятель-ность ответов (15)
3	3. Тема 3. Практические вопросы реализации Федерального закона «О персональных данных» от 27 июля 2006 года № 152-ФЗ	ПК-29	З.знать требования правовых актов в области защиты государственной тайны и информационной безопасности У.уметь соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, уметь обеспечивать соблюдение режима секретности Н.владеть навыками соблюдения в профессиональной	Практическая работа №3	14-15 баллов — сформированные систематические знания; на высоком уровне осуществляе-мые умения, успешно применяемые навыки; 11-13 баллов — сформированные, но содержа-щие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы уме-ния; в целом успешное, но содержащее отдельные

№ 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)
			деятельности требований правовых актов в области защиты государственной тайны и информационной безопасности		пробелы применение навыков; 7-10 баллов — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 6 и менее баллов — студент обнаружил несостоятель-ность ответов (15)
4	4. Тема 4. Нормативно-методическое обеспечение безопасности информационных систем персональных данных	ПК-29	З.знать требования правовых актов в области защиты государственной тайны и информационной безопасности У.уметь соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, уметь обеспечивать соблюдение режима секретности Н.владеть навыками соблюдения в профессиональной деятельности требований правовых актов в области защиты государственной тайны и информационной безопасности	Практическая работа №4	14-15 баллов — сформированные систематические знания; на высоком уровне осуществляе-мые умения, успешно применяемые навыки; 11-13 баллов — сформированные, но содержа-щие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы уме-ния; в целом успешное, но содержащее отдельные пробелы применение навыков; 7-10 баллов — общие, но не структурированные знания; не систематически осуществляемые 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; 6 и менее баллов — студент обнаружил несостоятель-ность ответов (15)
5	5. Тема 5. Специфика работы с персональными данными в организации (учреждении, предприятии)	ПСК-2	З.знать основные требования к обеспечению личной безопасности и безопасность граждан в процессе выполнения служебных задач У.уметь обеспечивать личную безопасность и безопасность граждан в процессе выполнения служебных задач Н.владеть навыками обеспечения личной безопасности и безопасности граждан в процессе выполнения служебных задач	Практическая работа №5	14-15 баллов — сформированные систематические знания; на высоком уровне осуществляе-мые умения, успешно применяемые навыки; 11-13 баллов — сформированные, но содержа-щие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы уме-ния; в целом успешное, но содержащее отдельные пробелы применение навыков; 7-10 баллов — общие, но не структурированн ые знания; не систематически осуществляемые умения; не систематически применяемые навыки; 6 и менее баллов — студент обнаружил несостоятель-ность ответов (15)
6	6. Тема 6.	ПСК-2	З.знать основные	Практическая работа	14-15 баллов —

№ 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)
	Методы защиты информационных систем персональных данных		требования к обеспечению личной безопасности и безопасность граждан в процессе выполнения служебных задач У.уметь обеспечивать личную безопасность и безопасность граждан в процессе выполнения служебных задач Н.владеть навыками обеспечения личной безопасности и безопасности граждан в процессе выполнения служебных задач	№6	сформированные систематические знания; на высоком уровне осуществляе-мые умения, успешно применяемые навыки; 11-13 баллов — сформированные, но содержа-щие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы уме-ния; в целом успешное, но содержащее отдельные пробелы применение навыков; 7-10 баллов — общие, но не структурированн ые знания; не систематически осуществляемые умения; не систематически применяемые навыки; 6 и менее баллов — студент обнаружил несостоятель-ность ответов (15)
7	7. Тема 7. Организация и обеспечение режимов защиты персональных данных	ПСК-2	З.знать основные требования к обеспечению личной безопасности и безопасность граждан в процессе выполнения служебных задач У.уметь обеспечивать личную безопасность и безопасность	Практическая работа №7	14-15 баллов — сформированные систематические знания; на высоком уровне осуществляе-мые умения, успешно применяемые навыки; 11-13 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)
			граждан в процессе выполнения служебных задач Н.владеть навыками обеспечения личной безопасности и безопасности граждан в процессе выполнения служебных задач		но содержа-щие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы уме-ния; в целом успешное, но содержащее отдельные пробелы применение навыков; 7-10 баллов — общие, но не структурированн ые знания; не систематически осуществляемые умения; не систематически применяемые навыки; 6 и менее баллов — студент обнаружил несостоятель-ность ответов (15)
				Итого	**100**

6.2. Промежуточный контроль (зачет, экзамен)

Рабочим учебным планом предусмотрен Зачет в семестре 31.

ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ:

1-й вопрос билета (30 баллов), вид вопроса: Тест/проверка знаний. Критерий: Максимальное количество баллов, которые может получить каждый студент за тест в относительных единицах равняется 30-ти. Каждый правильный ответ оценивается в 1 балл, полученный результат делится на общее количество вопросов в тесте и умножится на 30..

Компетенция: ПК-29 способность соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

Знание: знать требования правовых актов в области защиты государственной тайны и информационной безопасности

1. Вопрос автономии операторов в выборе мер защиты персональных данных
2. Информация о частной жизни граждан и персональные данные.
3. Обработка персональных данных третьим лицом в интересах оператора.
4. Обработка персональных данных: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (передача), обезличивание, блокирование, уничтожение.
5. Обязанности оператора персональных данных в ходе сбора и обработки персональных данных, ответы на запросы субъектов.
6. Основы законодательства в области персональных данных. Определение понятия «персональные данные».
7. Ответственность за нарушение требований по обращению с персональными данными.
8. Персональные данные в Федеральном законе и Трудовом кодексе Российской Федерации.
9. Понятие права на неприкосновенность частной жизни, его определение.
10. Порядок проведения классификации информационных систем персональных данных.
11. Практические вопросы исполнения операторами персональных данных своих обязанностей.
12. Руководящие документы ФСТЭК и ФСБ России по защите персональных данных. Нормативно-методическое обеспечение безопасности информационных систем персональных данных в органах власти, учреждениях (предприятиях).
13. Содержание категории «персональные данные».
14. Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных.
15. Характеристики информации о частной жизни гражданина.

Компетенция: ПСК-2 способность обеспечивать личную безопасность и безопасность граждан в процессе выполнения служебных задач

Знание: знать основные требования к обеспечению личной безопасности и безопасность граждан в процессе выполнения служебных задач

16. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
17. Биометрические персональные данные, специальные категории персональных данных.
18. Лицензирование деятельности по технической защите конфиденциальной информации при защите персональных данных. Основные требования для получения лицензии.
19. Локальные нормативные акты организации, составляемые с учетом требований Роскомнадзора в области защиты персональных данных
20. Модель злоумышленника информационных систем персональных данных.
21. Обезличенные персональные данные.
22. Ограничение доступа к персональным данным, учет лиц, допущенных к персональным данным, определение порядка обращения с такими сведениями, контроля над его соблюдением, организация доступа к персональным данным, внутренние нормативные документы по охране конфиденциальности сведений, их содержание, порядок разработки и ввода в действие, контроль над соблюдением режима конфиденциальности
23. Организационные и технические мероприятия, направленные на минимизацию ущерба от возможной реализации угроз безопасности персональных данных.
24. Организация защиты персональных данных обрабатываемых автоматизированным способом. Требования, методы и средства.
25. Организация защиты персональных данных обрабатываемых неавтоматизированным способом. Требования, методы и средства. Стратегия защиты персональных данных
26. Основные локальные нормативные акты для организации работы с персональными данными. Сферы их регулирования и структура.

27. Основные положения закона «О персональных данных» от 27 июля 2006 года № 152-ФЗ. Сфера регулирования. Категории персональных данных.
28. Основные принципы обработки персональных данных.
29. Ответственность операторов персональных данных.
30. Перечень необходимой информации для организации выполнения требований законодательства.
31. Порядок создания системы защиты персональных данных от несанкционированных воздействий по техническим каналам.
32. Права субъектов персональных данных и их соблюдение при обработке персональных данных.
33. Разработка частных моделей угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования.
34. Требования к операторам персональных данных.
35. Условия обработки персональных данных.

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: ПК-29 способность соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности
Умение: уметь соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, уметь обеспечивать соблюдение режима секретности
Задача № 1. Будет ли считаться персональными данными та информация, которую предоставляет клиент, заполняя в анкете на интернет-сайте специальные поля, указывая кроме фамилии, имени, отчества, места жительства, паспортных данных также сведения из других документов, относящихся к гражданину опосредованно?
Задача № 2. В каких случаях оператор вправе осуществлять обработку персональных данных без уведомления уполномоченного органа по защите прав субъектов персональных данных?
Задача № 3. Вправе ли кредитная организация обрабатывать персональные данные физических лиц, получивших отказ в предоставлении кредита? Возможно ли хранить формы анкет-заявок на получение кредита в формате цифровых копий?
Задача № 4. Для тех, кто ведет свой бизнес в Интернете, актуален вопрос о месте и стране обработки и хранения персональных данных. Можно ли хранить персональные данные за пределами России? Допускается ли при этом возможность поручить обработку этих данных третьему лицу (передать на аутсорсинг), в том числе находящемуся за границей?
Задача № 5. Как посетитель сайта может использовать свое право запросить информацию у оператора о ПДн, обрабатываемых на сайте?

Задача № 6. Как поступить в случае размещения недостоверной информации на сайтах госорганов в общедоступных реестрах?
Задача № 7. Можно ли признавать работу с файлами в форматах doc. и xls, расположенных в сетевом хранилище данных неавтоматизированной обработкой?
Задача № 8. Насколько правомерным является размещение плана проверочной деятельности на официальных сайтах контрольных органов, в котором есть сведения об индивидуальных предпринимателях, такие как: адреса места жительства, сведения о собственности и проч.?
Задача № 9. Нужно ли согласие на обработку ПДн родственников государственного служащего?
Задача № 10. Что является достаточным подтверждением согласия субъекта на обработку его персональных данных для практики ведения бизнеса в Интернете? Является ли таким согласием проставление им галочки при заполнении специальной анкеты на интернет-сайте для последующего оформления страхового полиса, банковской или иной услуги?
Задача № 11. Юридическое лицо поручает другому юридическому лицу собирать и обрабатывать ПДн субъектов. Кто в этом случае является оператором, и кто несет ответственность перед субъектом ПДн?

Компетенция: ПСК-2 способность обеспечивать личную безопасность и безопасность граждан в процессе выполнения служебных задач

Умение: уметь обеспечивать личную безопасность и безопасность граждан в процессе выполнения служебных задач
Задача № 12. Будет ли иметь юридическую силу согласие работника на передачу работодателем ПДн третьим лицам в коммерческих целях, подписанное простой электронной подписью, если работник и работодатель подпишут предварительное соглашение об использовании простой электронной подписи?
Задача № 13. Как получить согласия на обработку ПДн, которые вносятся в информационную систему, если источником этих ПДн являются визитки?
Задача № 14. Как узнать адрес проведения плановых проверок оператора ПДн в случае проведения проверки в компании, имеющей несколько филиалов в пределах одного региона?
Задача № 15. Может ли быть согласие работника единственным основанием для обработки его ПДн в целях, не предусмотренных для конкретного оператора? Например: Согласие работника в письменной форме сведений о его вероисповедании в нерелигиозных организация.
Задача № 16. Может ли письменное согласие на передачу ПДн работника третьим организациям не содержать указания конкретных операторов, которым передаются ПДн?
Задача № 17. Насколько правомерно получение согласия, в случае если это всплывающее окно с уведомлением об обработке ПДн (Google Analytics и Яндекс Метрика).
Задача № 18. Насколько правомерным является использование ПДн, полученных из общедоступных источников, в иных целях, отличных от целей их первоначального сбора?
Задача № 19. Нужно ли каждому филиалу иметь свою документацию по ПДн, или достаточно тех документов, которые в головном офисе?
Задача № 20. Нужно ли согласие на трансграничную передачу на территорию стран, являющимися сторонами Конвенции совета Европы?
Задача № 21. Распространяются ли действия ч.4 ст.9 Федерального закона № 152 ФЗ «О персональных данных» на положение ч.1 ст.8 того же закона о включении ПДн в общедоступный источник ПДн?
Задача № 22. Считается ли предоставление удаленного доступа иностранным компаниям в базы данных информационных систем персональных данных, расположенных на территории РФ трансграничной передачей ПДн?
Задача № 23. Является ли оператором лицо, действующее по поручению другого оператора?

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; 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; 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; 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: ПК-29 способность соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

Навык: владеть навыками соблюдения в профессиональной деятельности требований правовых актов в области защиты государственной тайны и информационной безопасности

Задание № 1. Определить актуальность угрозы с высокой возможностью реализации для ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъекты ПДн.

Задание № 2. Определить сертифицированные ФСТЭК межсетевые экраны, которые могут использоваться в ИСПДн для обеспечения 3 уровня защищенности.

Задание № 3. Определить сертифицированные ФСТЭК операционные системы, которые могут использоваться в ИСПДн для обеспечения 1 уровня защищенности.

Задание № 4. Определить сертифицированные ФСТЭК системы обнаружения вторжений и средства антивирусной защиты для обеспечения 2 уровня защищенности.

Задание № 5. Определить состав и содержание организационных и технических мер для обеспечения 3 уровня защищенности персональных данных при их обработке в информационных системах персональных данных.

Задание № 6. Определить состав и содержание организационных и технических мер для обеспечения 4 уровня защищенности персональных данных при их обработке в информационных системах персональных данных.

Задание № 7. Определить тип актуальных угроз для информационной системы обрабатывающей иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Задание № 8. Разработать порядок обращения с материальными носителями биометрических персональных данных в соответствии с Постановлением Правительства РФ от 6 июля 2008 г. N 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

Задание № 9. Составить документ определяющий порядок обработки персональных данных без использования средств автоматизации согласно Постановлению Правительства РФ от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Задание № 10. Составить форму согласия на обработку персональных данных в соответствии с ФЗ «О персональных данных»
Задание № 11. Составить форму уведомления об обработке оператором персональных данных в соответствии с ФЗ «О персональных данных».

Компетенция: ПСК-2 способность обеспечивать личную безопасность и безопасность граждан в процессе выполнения служебных задач

Навык: владеть навыками обеспечения личной безопасности и безопасности граждан в процессе выполнения служебных задач
Задание № 12. В соответствии с методикой ФСТЭК идентифицировать источники угроз безопасности информации для информационных систем, в которых целью защиты является обеспечение целостности и доступности обрабатываемой информации.
Задание № 13. В соответствии с методикой ФСТЭК определить возможные способы реализации угроз безопасности информации пользователями системы непреднамеренно из-за неосторожности или неквалифицированных действий.
Задание № 14. В соответствии с методикой ФСТЭК оценить возможности по реализации угроз безопасности информации внешних нарушителей, не имеющих права доступа к информационной системе, ее отдельным компонентам и реализующих угрозы безопасности информации из-за границ информационной системы.
Задание № 15. Описать возможности внешнего нарушителя, реализующего несанкционированный доступ к информационной системе персональных данных в соответствии с «Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК 15 февраля 2008 г.).
Задание № 16. Определить необходимый уровень защищенности персональных данных в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных» (утв. Постановлением Правительства РФ от 01.11.2012 N 1119). Исходные данные задаются преподавателем.
Задание № 17. Определить перечень угроз безопасности персональных данных, обрабатываемых в автоматизированных рабочих местах, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена в соответствии с «Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК 15 февраля 2008 г.).
Задание № 18. Определить перечень угроз безопасности персональных данных, обрабатываемых в локальных информационных системах персональных данных, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена в соответствии с «Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК 15 февраля 2008 г.).
Задание № 19. Определить перечень угроз безопасности персональных данных, обрабатываемых в распределенных информационных системах персональных данных, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена в соответствии с «Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК 15 февраля 2008 г.).
Задание № 20. Определить состав и содержание организационных и технических мер для обеспечения 1 и 2 уровней защищенности персональных данных при их обработке в информационных системах персональных данных.
Задание № 21. Определить тип угроз информационной системе в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных» (утв. Постановлением Правительства РФ от 01.11.2012 N 1119). Исходные данные задаются преподавателем.

Задание № 22. Определить уровень исходной защищённости информационной системы персональных данных (Y1) согласно «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК 14 февраля 2008 г.). Исходные данные задаются преподавателем.
Задание № 23. Определить частоту (вероятность) реализации рассматриваемой угрозы (Y2) в информационной системе персональных данных согласно «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК 14 февраля 2008 г.). Исходные данные задаются преподавателем.

ОБРАЗЕЦ БИЛЕТА

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

Направление - 37.05.02 Психология служебной деятельности
Профиль - Морально-психологическое обеспечение служебной деятельности
Кафедра математических методов и цифровых технологий
Дисциплина - Защита персональных данных

БИЛЕТ № 1

1. Тест (30 баллов).
2. Нужно ли согласие на трансграничную передачу на территорию стран, являющимися сторонами Конвенции совета Европы? (35 баллов).
3. Определить перечень угроз безопасности персональных данных, обрабатываемых в автоматизированных рабочих местах, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена в соответствии с «Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК 15 февраля 2008 г.). (35 баллов).

Составитель _____ М.М. Бусько

Заведующий кафедрой _____ С.С. Ованесян

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

а) основная литература:

1. 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.
2. Сачков Д. И., Быкова В. Н., Смирнова И. Г. Оценка уровня защищенности персональных данных в организациях. Электронный ресурс/ Д. И. Сачков, И. Г. Смирнова, В. Н. Быкова.- Иркутск: Изд-во БГУЭП, 2015.-148 с.
3. Воробьев Е.Г. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс] : учебное

пособие / Е.Г. Воробьев. — Электрон. текстовые данные. — СПб. : Интермедия, 2017. — 432 c. — 978-5-4383-0120-2. — Режим доступа: http://www.iprbookshop.ru/66796.html
4. Скрипник Д.А. Обеспечение безопасности персональных данных [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 121 c.— Режим доступа: http://www.iprbookshop.ru/52153.— ЭБС «IPRbooks»

б) дополнительная 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. Комплексная система защиты информации на предприятии. учеб. пособие для вузов. рек. УМО вузов РФ по образованию в обл. историко-архивоведения/ Н. В. Гришина.- М.: ФОРУМ, 2014.-238 с.
3. 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)
4. Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00. http://fstec.ru/component/attachments/download/489
5. Кухаренко Т.А. Комментарий к Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (3-е издание переработанное и дополненное) [Электронный ресурс]/ Кухаренко Т.А., Захарова Н.А.— Электрон. текстовые данные.— Саратов: Ай Пи Эр Медиа, 2016.— 151 c.— Режим доступа: http://www.iprbookshop.ru/49154.— ЭБС «IPRbooks»
6. Перечень средств защиты информации, сертифицированных ФСБ России. http://clsz.fsb.ru/files/download/svedenia_po_sertifikatam_(010717).doc
7. Петренко В.И. Защита персональных данных в информационных системах [Электронный ресурс] : учебное пособие / В.И. Петренко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 201 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66023.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

– Единое окно доступа к информационным ресурсам, адрес доступа: http://window.edu.ru/. доступ неограниченный

– 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

– 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

– 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: http://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:

– MS Office,

– Гарант платформа F1 7.08.0.163 - информационная справочная система,

– КонсультантПлюс: Версия Проф - информационная справочная система,

– КонсультантПлюс: Сводное региональное законодательство,

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,

– Мультимедийный класс,

– Компьютерный класс,

– Наборы демонстрационного оборудования и учебно-наглядных пособий