Министерство науки и высшего образования Российской Федерации

Муромский институт (филиал)

федерального государственного бюджетного образовательного учреждения высшего образования

«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»

(МИ ВлГУ)

Кафедра *Юриспруденции*

«УТВЕРЖДАЮ»
Заместитель директора по УР
_____Д.Е. Андрианов
25.05.2021

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Организационное и правовое обеспечение информационной безопасности

Направление подготовки *10.03.01 Информационная безопасность*

Профиль подготовки *Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)*

Семестр	Трудоемкость, час./зач. ед.	Лекции, час.	Практические занятия, час.	Лабораторные работы, час.	Консультация, час.	Контроль, час.	Всего (контактная работа), час.	СРС, час.	Форма промежуточного контроля (экз., зач., зач. с оц.)
7	**72 / 2**	**16**	**16**		**1,8**	**0,25**	**34,05**	**37,95**	**Зач.**
Итого	**72 / 2**	**16**	**16**		**1,8**	**0,25**	**34,05**	**37,95**	

Муром, 2020 г.

1. Цель освоения дисциплины

Цель курса – раскрыть основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации и механизм их реализации, понятия и виды защищаемой информации по законодательству РФ, систему защиты государственной тайны, основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности, а также понятие и виды компьютерных преступлений.

Задачи дисциплины – дать основы:

информационного законодательства Российской Федерации;

системы защиты государственной тайны;

правил лицензирования и сертификации в области защиты информации;

международного законодательства в области защиты информации;

знаний о компьютерных преступлениях.

2. Место дисциплины в структуре ОПОП ВО

Курс "Организационное и правовое обеспечение информационной безопасности" базируется на изучении дисциплин: "Основы информационной безопасности", "Теория информации", "Техническая защита информации» и служит базой дисциплины "Защита информации от утечки по техническим каналам".

3. Планируемые результаты обучения по дисциплине

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции	Результаты обучения по дисциплине	
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.1 Организует правовое обеспечение информационной безопасности	Уметь при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ОПК-6.1)	тест, вопросы к устному опросу
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы,	ОПК-5.2 Применяет нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере	Знать нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере	тест, вопросы к устному опросу

регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	профессиональной деятельности	профессиональной деятельности (ОПК-5.2)	

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

4.1. Форма обучения: очная

Уровень базового образования: среднее общее.
Срок обучения 4г.

4.1.1. Структура дисциплины

№ п\п	Раздел (тема) дисциплины	Семестр	Контактная работа обучающихся с педагогическим работником							Самостоятельная работа	Форма текущего контроля успеваемости (по неделям семестра), форма промежуточной аттестации(по семестрам)
			Лекции	Практические занятия	Лабораторные работы	Контрольные работы	КП / КР	Консультация	Контроль		
1	Общая часть	7	8	10						20	тестирование, устный опрос
2	Особенная часть	7	8	6						17,95	тестирование, устный опрос
Всего за семестр		72	16	16				1,8	0,25	37,95	Зач.
Итого		72	16	16				1,8	0,25	37,95	

4.1.2. Содержание дисциплины

4.1.2.1. Перечень лекций

Семестр 7

Раздел 1. Общая часть

Лекция 1.

Понятие и виды защищаемой информации по законодательству РФ (2 часа).

Лекция 2.

Субъекты и объекты правоотношений в области информационной безопасности (2 часа).

Лекция 3.

Понятие, сущность, цели и значение защиты конфиденциальной информации (2 часа).

Лекция 4.

Правовое режимы защиты конфиденциальной информации (2 часа).

Раздел 2. Особенная часть

Лекция 5.

Основные требования, предъявляемые к организации защиты конфиденциальной информации (2 часа).

Лекция 6.

Юридическая ответственность за нарушение правового режима конфиденциальной информации (2 часа).

Лекция 7.

Правовой режим государственной тайны (2 часа).

Лекция 8.

Порядок допуска и доступа к государственной тайне (2 часа).

4.1.2.2. Перечень практических занятий

Семестр 7

Раздел 1. Общая часть

Практическое занятие 1

Законодательство в области информационной безопасности (2 часа).

Практическое занятие 2

Понятие, сущность, цели и значение защиты конфиденциальной информации (2 часа).

Практическое занятие 3

Основные требования, предъявляемые к организации защиты конфиденциальной информации (2 часа).

Практическое занятие 4

Правовой режим государственной тайны (2 часа).

Практическое занятие 5

Правовой режим защиты коммерческой тайны (2 часа).

Раздел 2. Особенная часть

Практическое занятие 6

Государственное регулирование деятельности по лицензированию и сертификации в области информационной безопасности (2 часа).

Практическое занятие 7

Проблемы защиты интеллектуальной собственности (2 часа).

Практическое занятие 8

Служба безопасности объекта. Организация и обеспечение режима секретности (2 часа).

4.1.2.3. Перечень лабораторных работ

Не планируется.

4.1.2.4. Перечень тем и учебно-методическое обеспечение самостоятельной работы

Перечень тем, вынесенных на самостоятельное изучение:

1. Понятие и способы защиты интеллектуальных прав.
2. Типы договоров в области защиты информации.
3. Особенности трудовых соглашений в области защиты информации.
4. Система лицензирования в области защиты конфиденциальной информации.
5. Система сертификации средств защиты информации.
6. Понятие и объекты стандартизации средств защиты информации.
7. Правовая защита компьютерной информации, содержание компьютерной информации.
8. Понятие и классификация видов компьютерных правонарушений.
9. Уголовно-правовая и криминалистическая характеристика компьютерных правонарушений.
10. Способы и механизмы совершения компьютерных правонарушений.
11. Понятие и виды юридической ответственности за нарушение правовых норм в области информационной безопасности.
12. Уголовная ответственность за нарушение правовых норм в сфере информационной безопасности.
13. Административная ответственность за нарушение правовых норм в сфере информационной безопасности.
14. Особенности юридической ответственности за нарушение правовых норм информационной безопасности в области трудовых и гражданско-правовых отношений.

Для самостоятельной работы используются методические указания по освоению дисциплины и издания из списка приведенной ниже основной и дополнительной литературы.

4.1.2.5. Перечень тем контрольных работ

Не планируется.

4.1.2.6. Примерный перечень тем курсовых работ

Не планируется.

5. Образовательные технологии

Для освоения бакалаврами учебной дисциплины, получения знаний и формирования профессиональных компетенций используются следующие образовательные технологии:

- лекция с элементами дискуссии, постановкой проблем;
- комментирование ответов студентов;
- решение задач;
- анализ конкретных ситуаций;
- составление таблиц и схем;
- тестирование.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Фонды оценочных материалов (средств) приведены в приложении.

7. Учебно-методическое и информационное обеспечение дисциплины.

7.1. Основная учебно-методическая литература по дисциплине

1. Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Москва: ЮНИТИ-ДАНА, 2017. — 287 c. — ISBN 978-5-238-02857-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/72444.html — Режим доступа: для авторизир. пользователей. - https://www.iprbookshop.ru/72444.html

2. Прохорова О.В. Информационная безопасность и защита информации: учебник / О. В. Прохорова. — Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 113 с. — ISBN 978-5-9585-0603-3. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/43183.html — Режим доступа: для авторизир. пользователей. - https://www.iprbookshop.ru/43183.html

3. Организационно-правовое обеспечение информационной безопасности: учебник / А.А. Стрельцов, В. Н. Пожарский, В. А. Минаев [и др.] ; под редакцией А. А. Александрова, М. П. Сычева. — Москва: Московский государственный технический университет имени Н.Э. Баумана, 2018. — 292 с. — ISBN 978-5-7038-4723-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/110777.html — Режим доступа: для авторизир. пользователей - https://www.iprbookshop.ru/33857.html

7.2. Дополнительная учебно-методическая литература по дисциплине

1. Филиппов Б.И. Информационная безопасность. Основы надежности средств связи: учебник / Б. И. Филиппов, О. Г. Шерстнева. — Саратов: Ай Пи Эр Медиа, 2019. — 227 c. — ISBN 978-5-4486-0485-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/80290.html — Режим доступа: для авторизир. пользователей. - https://www.iprbookshop.ru/80290.html

2. Морозов А.В. Информационное право и информационная безопасность. Часть 1: учебник для магистров и аспирантов / А.В. Морозов, Л.В. Филатова, Т.А. Полякова. — Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016. — 436 c. — ISBN 978-5-00094-296-3. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/72395.html — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/72395 - https://www.iprbookshop.ru/72395.html

3. Морозов А.В. Информационное право и информационная безопасность. Часть 2: учебник для магистров и аспирантов / А. В. Морозов, Л. В. Филатова, Т. А. Полякова. — Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016. — 604 с. — ISBN 978-5-00094-297-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/66771.html — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/66771 - https://www.iprbookshop.ru/66771.html

7.3. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

В образовательном процессе используются информационные технологии, реализованные на основе информационно-образовательного портала института (www.mivlgu.ru/iop), и инфокоммуникационной сети института:

- предоставление учебно-методических материалов в электронном виде;
- взаимодействие участников образовательного процесса через локальную сеть института и Интернет;
- предоставление сведений о результатах учебной деятельности в электронном личном кабинете обучающегося.

Информационные справочные системы:

Информационно-поисковая система Консультант Плюс (http://www.consultant.ru)

elibrary.ru - Научная электронная библиотека

Информационно-аналитический портал ISO27000.RU / ЗАЩИТА-ИНФОРМАЦИИ.SU (http://iso27000.ru)

Каталог решений и услуг по Информационной Безопасности (http://www.ru-ib.ru)

Программное обеспечение:

Не предусмотрено.

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

iprbookshop.ru
consultant.ru
iso27000.ru
ru-ib.ru
mivlgu.ru/iop

8. Материально-техническое обеспечение дисциплины

Лекционная аудитория

Экран Lumien, проектор в комплекте Sanyo PDG-DSU20

9. Методические указания по освоению дисциплины

Для успешного освоения теоретического материала обучающийся: знакомится со списком рекомендуемой основной и дополнительной литературы; уточняет у преподавателя, каким дополнительным пособиям следует отдать предпочтение; ведет конспект лекций и прорабатывает лекционный материал, пользуясь как конспектом, так и учебными пособиями.

На практических занятиях пройденный теоретический материал подкрепляется решением ситуационных задач и тестовых заданий по основным темам дисциплины.

Самостоятельная работа оказывает важное влияние на формирование личности будущего специалиста, она планируется обучающимся самостоятельно. Каждый обучающийся самостоятельно определяет режим своей работы и меру труда, затрачиваемого на овладение учебным содержанием дисциплины. Он выполняет внеаудиторную работу и изучение

разделов, выносимых на самостоятельную работу, по личному индивидуальному плану, в зависимости от его подготовки, времени и других условий.

Форма заключительного контроля при промежуточной аттестации – зачет. Для проведения промежуточной аттестации по дисциплине разработаны фонд оценочных средств и балльно-рейтинговая система оценки учебной деятельности студентов. Оценка по дисциплине выставляется в информационной системе и носит интегрированный характер, учитывающий результаты оценивания участия студентов в аудиторных занятиях, качества и своевременности выполнения заданий в ходе изучения дисциплины и промежуточной аттестации.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению *10.03.01 Информационная безопасность* и профилю подготовки *Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)*
Рабочую программу составил *к.ю.н., доцент Петрухина А.Н.*_____

Программа рассмотрена и одобрена на заседании кафедры *Юриспруденции*

протокол № 15 от 18.05.2021 года.
Заведующий кафедрой *Юриспруденции* _____*Каткова Л.В.*
(Подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии ФИТР

протокол № 9 от 24.05.2021 года.
Председатель комиссии ФИТР _____ *Рыжкова М.Н.*
(Подпись) (Ф.И.О.)

Приложение

Фонд оценочных материалов (средств) по дисциплине

Организационное и правовое обеспечение информационной безопасности

1. Оценочные материалы для проведения текущего контроля успеваемости по дисциплине

Рейтинг-контроль 1

Задания

Задание 1.

Проанализируйте конкретные ситуации и определите, в каких случаях нарушается право граждан на информацию.

– В анкете представленной куратором для заполнения студентами первого курса в числе других вопросов содержались, в частности, вопросы о родителях: «Фамилия, имя, отчество, домашний адрес, номер телефона, сведения о судимости, источник получения средств существования, принадлежность к политическим партиям».

– При приёме на работу в ювелирный отдел магазина работодатель запросил в соответствующих государственных органах сведения о судимости кандидата на должность, а также данные о наличии внебрачных связей.

– При допросе Петрова, подозреваемого в совершении экономического преступления, он отказался сообщать следствию информацию о доходах своей жены.

– У депутата Государственной Думы потребовали сведения о до- ходах, полученных им и членами его семьи за истекший год, а также о расходах, превышающих полученные за год доходы и об источниках их получения.

Решить (на основе нормативных актов) любые 2 ситуации, приведенные ниже:

Задание № 2

Определите, соответствуют ли ситуации, представленные ниже, принципам правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

1. В предисловии к роману писателя Зарецкого Н.К. коротко была изложена биография автора, где были собраны сведения из его жизни, они соответствовали действительности, однако до их публикации у автора не было получено разрешение автора.

2. После проведения аудиторской проверки в государственной организации было выявлено нецелевое использование бюджетных средств. Местные средства массовой информации подготовили публикацию об использовании бюджетных средств, однако руководитель организации запретил публиковать данную информацию.

3. На заводе, выпускающем радиоактивные металлы, произошла авария. Возникла реальная опасность радиоактивного заражения находящегося на расстоянии десяти километров от завода посёлка. Глава местной администрации, опасаясь паники среди населения, запретил до проведения анализа сообщать в средствах массовой ин- формации об аварии.

Рейтинг-контроль 2

Задания

1. СВЕДЕНИЯ (СООБЩЕНИЯ, ДАННЫЕ) НЕЗАВИСИМО ОТ ФОРМЫ ИХ ПРЕДСТАВЛЕНИЯ:

1. Информация
2. Информационные технологии
3. Информационная система
4. Информационно-телекоммуникационная сеть
5. Обладатель информации

2. ПРОЦЕССЫ, МЕТОДЫ ПОИСКА, СБОРА, ХРАНЕНИЯ, ОБРАБОТКИ, ПРЕДОСТАВЛЕНИЯ, РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ И СПОСОБЫ ОСУЩЕСТВЛЕНИЯ ТАКИХ ПРОЦЕССОВ И МЕТОДОВ:

1. Информация
2. Информационные технологии
3. Информационная система
4. Информационно-телекоммуникационная сеть
5. Обладатель информации

3. ЛИЦО, САМОСТОЯТЕЛЬНО СОЗДАВШЕЕ ИНФОРМАЦИЮ ЛИБО ПОЛУЧИВШЕЕ НА ОСНОВАНИИ ЗАКОНА ИЛИ ДОГОВОРА ПРАВО РАЗРЕШАТЬ ИЛИ ОГРАНИЧИВАТЬ ДОСТУП К ИНФОРМАЦИИ:

1. Источник информации
2. Потребитель информации
3. Уничтожитель информации
4. Носитель информации
5. Обладатель информации

5. ТЕХНОЛОГИЧЕСКАЯ СИСТЕМА, ПРЕДНАЗНАЧЕННАЯ ДЛЯ ПЕРЕДАЧИ ПО ЛИНИЯМ СВЯЗИ ИНФОРМАЦИИ, ДОСТУП К КОТОРОЙ ОСУЩЕСТВЛЯЕТСЯ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ЭТО:

1. База данных
2. Информационная технология
3. Информационная система
4. Информационно-телекоммуникационная сеть
5. Медицинская информационная система

6. ОБЯЗАТЕЛЬНОЕ ДЛЯ ВЫПОЛНЕНИЯ ЛИЦОМ, ПОЛУЧИВШИМ ДОСТУП К ОПРЕДЕЛЕННОЙ ИНФОРМАЦИИ, ТРЕБОВАНИЕ НЕ ПЕРЕДАВАТЬ ТАКУЮ ИНФОРМАЦИЮ ТРЕТЬИМ ЛИЦАМ БЕЗ СОГЛАСИЯ ЕЕ ОБЛАДАТЕЛЯ ЭТО:

1. Электронное сообщение
2. Распространение информации
3. Предоставление информации
4. Конфиденциальность информации
5. Доступ к информации

7. ДЕЙСТВИЯ, НАПРАВЛЕННЫЕ НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННЫМ КРУГОМ ЛИЦ ИЛИ ПЕРЕДАЧУ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННОМУ КРУГУ ЛИЦ ЭТО:

1. Уничтожение информации
2. Распространение информации
3. Предоставление информации
4. Конфиденциальность информации
5. Доступ к информации

8. ВОЗМОЖНОСТЬ ПОЛУЧЕНИЯ ИНФОРМАЦИИ И ЕЕ ИСПОЛЬЗОВАНИЯ ЭТО:

1. Сохранение информации
2. Распространение информации
3. Предоставление информации
4. Конфиденциальность информации
5. Доступ к информации

9. ИНФОРМАЦИЯ, ПЕРЕДАННАЯ ИЛИ ПОЛУЧЕННАЯ ПОЛЬЗОВАТЕЛЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ:

1. Электронное сообщение
2. Информационное сообщение
3. Текстовое сообщение
4. Визуальное сообщение
5. SMS-сообщение

10. ВСЕ КОМПОНЕНТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ, В КОТОРОМ НАКАПЛИВАЮТСЯ И ОБРАБАТЫВАЮТСЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ЭТО:

1. Информационная система персональных данных
2. База данных
3. Централизованное хранилище данных
4. Система Статэкспресс
5. Сервер

11. К СВЕДЕНИЯМ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА, СОГЛАСНО УКАЗУ ПРЕЗИДЕНТА РФ ОТ 6 МАРТА 1997 Г., ОТНОСЯТСЯ:

1. Информация о распространении программ
2. Информация о лицензировании программного обеспечения
3. Информация, размещаемая в газетах, Интернете
4. Персональные данные
5. Личная тайна

12. ОТНОШЕНИЯ, СВЯЗАННЫЕ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ, РЕГУЛИРУЮТСЯ ЗАКОНОМ…

1. «Об информации, информационных технологиях»
2. «О защите информации»
3. Федеральным законом «О персональных данных»
4. Федеральным законом «О конфиденциальной информации»
5. «Об утверждении перечня сведений конфиденциального характера»

13. ДЕЙСТВИЯ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ (СОГЛАСНО ЗАКОНУ), ВКЛЮЧАЯ СБОР, СИСТЕМАТИЗАЦИЮ, НАКОПЛЕНИЕ, ХРАНЕНИЕ, ИСПОЛЬЗОВАНИЕ, РАСПРОСТРАНЕНИЕ И Т. Д ЭТО:

1. «Исправление персональных данных»
2. «Работа с персональными данными»
3. «Преобразование персональных данных»
4. «Обработка персональных данных»
5. «Изменение персональных данных»

14. ДЕЙСТВИЯ, В РЕЗУЛЬТАТЕ КОТОРЫХ НЕВОЗМОЖНО ОПРЕДЕЛИТЬ ПРИНАДЛЕЖНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ КОНКРЕТНОМУ СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ:

1. Выделение персональных данных
2. Обеспечение безопасности персональных данных
3. Деаутентификация
4. Деавторизация
5. Деперсонификация

15. ПО РЕЖИМУ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПОДРАЗДЕЛЯЮТСЯ НА:

1. Многопользовательские
2. Однопользовательские

3. Без разграничения прав доступа
4. С разграничением прав доступа
5. Системы, не имеющие подключений

16. ПРОЦЕСС СООБЩЕНИЯ СУБЪЕКТОМ СВОЕГО ИМЕНИ ИЛИ НОМЕРА, С ЦЕЛЬЮ ПОЛУЧЕНИЯ ОПРЕДЕЛЁННЫХ ПОЛНОМОЧИЙ (ПРАВ ДОСТУПА) НА ВЫПОЛНЕНИЕ НЕКОТОРЫХ (РАЗРЕШЕННЫХ ЕМУ) ДЕЙСТВИЙ В СИСТЕМАХ С ОГРАНИЧЕННЫМ ДОСТУПОМ:

1. Авторизация
2. Аутентификация
3. Обезличивание
4. Деперсонализация
5. Идентификация

17. ПРОЦЕДУРА ПРОВЕРКИ СООТВЕТСТВИЯ СУБЪЕКТА И ТОГО, ЗА КОГО ОН ПЫТАЕТСЯ СЕБЯ ВЫДАТЬ, С ПОМОЩЬЮ НЕКОЙ УНИКАЛЬНОЙ ИНФОРМАЦИИ:

1. Авторизация
2. Обезличивание
3. Деперсонализация
4. Аутентифика́ция
5. Идентификация

18. ПРОСТЕЙШИМ СПОСОБОМ ИДЕНТИФИКАЦИИ В КОМПЬЮТЕРНОЙ СИСТЕМЕ ЯВЛЯЕТСЯ ВВОД ИДЕНТИФИКАТОРА ПОЛЬЗОВАТЕЛЯ, КОТОРЫЙ ИМЕЕТ СЛЕДУЮЩЕЕ НАЗВАНИЕ:

1. Токен
2. Password
3. Пароль
4. Login
5. Смарт-карта

19. ОСНОВНОЕ СРЕДСТВО, ОБЕСПЕЧИВАЮЩЕЕ КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ, ПОСЫЛАЕМОЙ ПО ОТКРЫТЫМ КАНАЛАМ ПЕРЕДАЧИ ДАННЫХ, В ТОМ ЧИСЛЕ – ПО СЕТИ ИНТЕРНЕТ:

1. Идентификация
2. Аутентификация
3. Авторизация
4. Экспертиза
5. Шифрование

20. НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ ЭТО:

1. Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально
2. Работа на чужом компьютере без разрешения его владельца
3. Вход на компьютер с использованием данных другого пользователя
4. Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей
5. Доступ к СУБД под запрещенным именем пользователя

21. «ПЕРСОНАЛЬНЫЕ ДАННЫЕ» ЭТО:

1. Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу
2. Фамилия, имя, отчество физического лица
3. Год, месяц, дата и место рождения, адрес физического лица

4. Адрес проживания физического лица
5. Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»

22. В ДАННОМ СЛУЧАЕ СОТРУДНИК УЧРЕЖДЕНИЯ МОЖЕТ БЫТЬ ПРИВЛЕЧЕН К ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:
1. Выход в Интернет без разрешения администратора
2. При установке компьютерных игр
3. В случаях установки нелицензионного ПО
4. В случае не выхода из информационной системы
5. В любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности

23. ПРОЦЕДУРА, ПРОВЕРЯЮЩАЯ, ИМЕЕТ ЛИ ПОЛЬЗОВАТЕЛЬ С ПРЕДЪЯВЛЕННЫМ ИДЕНТИФИКАТОРОМ ПРАВО НА ДОСТУП К РЕСУРСУ ЭТО:
1. Идентификация
2. Аутентификация
3. Стратификация
4. Регистрация
5. Авторизация

24. ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ, ДОСТУП К КОТОРОЙ ОГРАНИЧИВАЕТ В СООТВЕТСТВИИ С ЗАКОНАДЕЛЬСТВОМ РФ:
1. Информация составляющая государственную тайну
2. Информация составляющая коммерческую тайну
3. Персональная
4. Конфиденциальная информация
5. Документированная информация

25. ДЛЯ ТОГО ЧТОБЫ СНИЗИТЬ ВЕРОЯТНОСТЬ УТРАТЫ ИНФОРМАЦИИ НЕОБХОДИМО:
1. Регулярно производить антивирусную проверку компьютера
2. Регулярно выполнять проверку жестких дисков компьютера на наличие ошибок
3. Регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты)
4. Защитить вход на компьютер к данным паролем
5. Проводить периодическое обслуживание ПК

26. ПАРОЛЬ ПОЛЬЗОВАТЕЛЯ ДОЛЖЕН
1. Содержать цифры и буквы, знаки препинания и быть сложным для угадывания
2. Содержать только цифры
3. Содержать только буквы
4. Иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.)
5. Быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д.

27. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЕСПЕЧИВАЕТ…
1. Блокирование информации
2. Искажение информации
3. Сохранность информации
4. Утрату информации
5. Подделку информации

28. ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ «О ГОСУДАРСТВЕННОЙ ТАЙНЕ» БЫЛ ПРИНЯТ В СЛЕДУЮЩЕМ ГОДУ:

1. 1982
2. 1985
3. 1988
4. 1993
5. 2005

Рейтинг-контроль 3

Задания

1. С 21 января по 19 апреля 2009 года профессиональный программист Ершов А. незаконным путем добыл логины и пароли для доступа в сеть Интернет нескольких пользователей, провайдером которых является ОАО «ЦентрТелеком». Информация о логинах и паролях законных пользователей Интернет является коммерческой тайной ОАО «ЦентрТелеком». Получить пароли Ершову А. удалось с помощью системного администратора ОАО «ЦентрТелеком» Петрова Д., пользуясь его доверием. Ершов часто помогал профессиональными советами Петрову Д. и несколько раз оставался один за компьютером Петрова. Ершов А. с помощью добытого кода по ночам заходил в сеть Интернет, а на счета потерпевших списывались денежные суммы за пользование сетью Интернет в указанное время. За указанный период законные пользователи понесли убытки в сумме более 14 000 рублей.

Чьи права в данном случае нарушены? Какие права нарушены? Какая ответственность и за какие нарушения возникает?

2. Пешкин Н.Р. работал в должности инженера-программиста на телефонном заводе. Его компьютер был подключен с помощью модема к телефонной линии. Пешкин Н.Р. скопировал из Интернета программу типа "троянский конь", имитирующую нормальную работу ЭВМ и одновременно негласно для пользователя предоставляющую полный доступ к компьютеру. Эту программу Пешкин Н.Р. направил в виде текстового документа на электронный адрес Регионального управления федеральной почтовой связи (РУФПС). Когда пользователь на компьютере РУФПС открыл данный документ, сработала программа «троянский конь», при работе которой пользователь РУФПС не подозревал о ее существовании, а программа предоставляла Пешкину возможность просматривать и копировать на свой компьютер всю информацию, имеющуюся на компьютере РУФПС. Пешкин во время подключения компьютера РУФПС к сети Интернет, зашел на жесткий диск законного пользователя с целью скопировать два файла с паролями РУФПС, и просмотрев его содержимое скопировал из каталога C:\WINDOWS два файла: - user.dat и имя.pwl, на свой компьютер, принадлежащий конструкторскому бюро телефонного завода. После копирования данных файлов, Пешкин записал эти файлы вместо таких же на своем компьютере, принадлежащем конструкторскому бюро телефонного завода и, с помощью программы определения паролей, определил пароль подключения к сети Интернет РУФПС, с целью его дальнейшего использования, то есть подключения к сети Интернет за счет РУФПС. Совершив вышеуказанные действия Пешкин, зная имя и пароль РУФПС, в период с 4 декабря 2008 года по 5 февраля 2000 года систематически подключался к сети Интернет за счет РУФПС, чем причинил материальный ущерб РУФПС на сумму более 2900 рублей.

Чьи права в данном случае нарушены? Какие права нарушены? Какая ответственность и за какие нарушения возникает?

3. Картину Дуненко «Осень» купил Петров. Спустя год Дуненко обратился к Петрову с просьбой предоставить ему возможность снять копию с картины. Однако последний в просьбе отказал, сославшись на то, что выставляет через несколько дней картину для продажи на аукционе. На аукционе картина имела успех и была продана по цене, значительно превышающей предыдущую. Дуненко потребовал о Петрова уплатить причитающуюся ему долю от продажной цены картины. Однако тот отказался, заявив, что расплатился с ним полностью при покупке картины.

Правомерна ли просьба Дуненко о предоставлении ему собственником картины Петровым возможности снятия копии с проданной картины, и если да, как называется такое право? В каком случае Дуненко имеет право требовать от продавца написанной им картины вознаграждения после ее продажи. Как такое право называется? Как следует исчислять вознаграждение автору при перепродаже созданного им произведения? Какие действия должен предпринять Дуненко для осуществления права следования?

4. Индивидуальный предприниматель Жильцов А.А. умер. Он являлся единоличным автором двух программных продуктов «Fox» и «Ling», которые пользовались большим спросом на рынке ПО в области игровых программ. При жизни Жильцов А.А. не передавал права на данные программные продукты, у него нет наследников и он не оставил завещания.

Кому после смерти Жильцова А.А. перейдут личные неимущественные и исключительные права на данные программные продукты? Каковы сроки действия этих прав на указанное ПО?

Общее распределение баллов текущего контроля по видам учебных работ для студентов

Рейтинг-контроль 1	промежуточный тест	до 20 баллов
Рейтинг-контроль 2	промежуточный тест	до 20 баллов
Рейтинг-контроль 3	промежуточный тест	до 20 баллов
Посещение занятий студентом	отсутствие пропусков по неуважительным причинам	до 10 баллов
Дополнительные баллы (бонусы)	активность на занятиях	до 10 баллов
Выполнение семестрового плана самостоятельной работы	устный опрос	до 20 баллов

2. Промежуточная аттестация по дисциплине

Перечень вопросов к экзамену / зачету / зачету с оценкой.
Перечень практических задач / заданий к экзамену / зачету / зачету с оценкой (при наличии)

ОПК-5

Блок 1 (знать)

1. Основные понятия, виды и источники информации, подлежащие защите.
2. Свойства информации.
3. Принципы правового регулирования общественных отношений в информационной сфере.
4. Правомочия субъектов в области защиты информации.
5. Понятие защиты информации и ее сущность.
6. Способы защиты информации.
7. Классификация правовых режимов информации.
8. Общедоступная информация.
9. Распространение информации и ограничение доступа к информации.
10. Источники, содержащие конфиденциальную информацию.

Задания

Определите, соответствуют ли ситуации, представленные ниже, принципам правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

1. В предисловии к роману писателя Зарецкого Н.К. коротко была изложена биография автора, где были собраны сведения из его жизни, они соответствовали действительности, однако до их публикации у автора не было получено разрешение автора.
2. После проведения аудиторской проверки в государственной организации было выявлено нецелевое использование бюджетных средств. Местные средства массовой информации подготовили публикацию об использовании бюджетных средств, однако руководитель организации запретил публиковать данную информацию.
3. На заводе, выпускающем радиоактивные металлы, произошла авария. Возникла реальная опасность радиоактивного заражения находящегося на расстоянии десяти километров от завода посёлка. Глава местной администрации, опасаясь паники среди населения, запретил до проведения анализа сообщать в средствах массовой ин- формации об аварии.

ОПК-6:

Блок 1 (Знать)

Информационная безопасность в системе национальной безопасности РФ.

12. Методы, формы и средства обеспечения информационной безопасности.
13. Основные направления деятельности государства и принципы обеспечения информационной безопасности.
14. Субъекты, обеспечивающие защиту государственных информационных ресурсов.
15. Субъекты информационных правоотношений в области государственной тайны.
16. Принципы и основания отнесения сведений к государственной тайне.
17. Определение сведений, составляющих коммерческую тайну.
18. Объекты защиты коммерческой тайны.
19. Организация защиты коммерческой тайны.
20. Понятие и способы защиты интеллектуальных прав.
21. Типы договоров в области защиты информации.
22. Особенности трудовых соглашений в области защиты информации.
23. Система лицензирования в области защиты конфиденциальной информации.
24. Система сертификации средств защиты информации.
25. Понятие и объекты стандартизации средств защиты информации.
26. Правовая защита компьютерной информации, содержание компьютерной информации.
27. Понятие и классификация видов компьютерных правонарушений.
28. Уголовно-правовая и криминалистическая характеристика компьютерных правонарушений.
29. Способы и механизмы совершения компьютерных правонарушений.
30. Понятие и виды юридической ответственности за нарушение правовых норм в области информационной безопасности.
31. Уголовная ответственность за нарушение правовых норм в сфере информационной безопасности.
32. Административная ответственность за нарушение правовых норм в сфере информационной безопасности.
33. Особенности юридической ответственности за нарушение правовых норм информационной безопасности в области трудовых и гражданско-правовых отношений.

Задания

1. Министерство обороны России обвинило редакцию журнала «Власть» в разглашении государственной тайны. Журнал опубликовал справочные материалы, содержащие, по мнению военных чиновников, сведения, спрятанные под грифом «совершенно секретно». По словам журналистов, информация взята исключительно из открытых источников, более того, большая часть данных опубликована в свободном доступе в сети Интернет на официальных

сайтах органов власти. Для доказательства своей правоты редакция готова продемонстрировать распечатки страниц официальных сайтов и копии газетных публикаций.

Может ли относиться к государственной тайне информация, размещенная в открытом доступе? Кому в этом случае нужно предъявлять обвинения?

2. Сергей Васильев в период с ноября 1994 года по август 2001 года проходил военную службу на различных должностях в воинских частях, дислоцированных в Молдове. Полагая, что за этот период военной службы денежное содержание подлежало выплате ему в иностранной валюте, он просил произвести перерасчет и взыскать задолженность по денежному содержанию. Для этого он обратился с иском в гарнизонный военный суд.

Определением судьи указанного суда исковое заявление ввиду его неподсудности данному суду возвращено заявителю. При этом в определении указывалось, что, поскольку вопросы выплаты денежного содержания военнослужащим, проходящим военную службу на территории иностранного государства, регулируются секретными постановлениями Правительства Российской Федерации, то рассмотрение данного спора подсудно окружному военному суду.

Не соглашаясь с вынесенным определением, представитель истца в частной жалобе просил определение отменить и направить исковое заявление для рассмотрения в тот же суд. Свои действия он мотивировал тем, что указанные в исковом заявлении положения нормативных актов в части, касающейся порядка денежного обеспечения военнослужащих, проходящих военную службу на территории иностранного государства, не могут быть отнесены к сведениям, составляющим государственную тайну.

Кто прав в данном случае? Относятся ли упомянутые сведения к государственной тайне? В каком суде должно рассматриваться данное дело?

Методические материалы, характеризующие процедуры оценивания

При проведении промежуточной аттестации с зачетом и общей суммой 100 баллов, баллы формируются в процессе 3-х промежуточных рейтингов, исходя из установленного максимума. При получении по сумме трех рейтингов 60 баллов и более, студент имеет право на получение зачета.

Максимальная сумма баллов, набираемая студентом по дисциплине равна 100.

Оценка в баллах	Оценка по шкале	Обоснование	***Уровень сформированности компетенций***
Более 80	«Отлично»	Содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному	***Высокий уровень***
66-80	«Хорошо»	Содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом	***Продвинутый уровень***

		сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками	
50-65	«Удовлетворительно»	Содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки	***Пороговый уровень***
Менее 50	«Неудовлетворительно»	Содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки	***Компетенции не сформированы***

3. Задания в тестовой форме по дисциплине

Примеры заданий:

1. В соответствии с Конституцией Российской Федерации информация и связь относятся:

а) к исключительному ведению Российской Федерации;

б) к совместному ведению Российской Федерации и субъектов Российской Федерации;

в) к ведению субъектов Российской Федерации.

г) к совместному ведению организаций и граждан в том числе зарубежных стран

Полный перечень тестовых заданий с указанием правильных ответов, размещен в банке вопросов на информационно-образовательном портале института по ссылке https://www.mivlgu.ru/iop/question/edit.php?courseid=2216&cat=38520%2C66126&category=36809%2C66126&qbshowtext=0&recurse=0&recurse=1&showhidden=0

Оценка рассчитывается как процент правильно выполненных тестовых заданий из их общего числа.