МИНОБРНАУКИ РОССИИ

Ярославский государственный университет им. П.Г. Демидова

Кафедра интеллектуальных информационных радиофизических систем

|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ  Декан физического факультета  И.С. Огнев  *(подпись)*  «21» мая 2024 г. |

**Рабочая программа дисциплины**

**«Правовые основы информационной безопасности»**

Направление подготовки

11.03.01 Радиотехника

Направленность (профиль)

«Радиотехника»

Форма обучения

очная

|  |  |
| --- | --- |
| Программа рассмотрена  на заседании кафедры  от «29» марта 2024 года, протокол № 6 | Программа одобрена НМК  физического факультета  протокол № 5 от «30» апреля 2024 года |

**1. Цели освоения дисциплины**

Целями освоения дисциплины «Правовые основы информационной безопасности» являются формирование способности самостоятельно приобретать и использовать в профессиональной деятельности новые знания в области правовых основ информационной безопасности, используя современные образовательные и информационные технологии.

Курс знакомит с основными нормативными документами в области информационной безопасности личности, государства, общества, бизнеса, основами информационной защиты электронного документооборота и информационных систем различного назначения, с мерами ответственности за правонарушения в области информационной безопасности.

Задачи курса – способствовать формированию у студентов навыка самостоятельного приобретения новых знаний и профессиональной деятельности в области информационной безопасности в правовом поле.

**2. Место дисциплины в структуре образовательной программы**

Данная дисциплина является факультативной дисциплиной.

Дисциплина требует знаний, умений и навыков, полученных при изучении дисциплины «Правоведение». Знания, умения и навыки, полученные при изучении дисциплины, используются студентами при изучении специальных дисциплин и в НИРС.

**3. Планируемые результаты обучения по дисциплине, соотнесённые с планируемыми результатами освоения образовательной программы**

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ОП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

|  |  |  |
| --- | --- | --- |
| **Формируемая компетенция**  **(код и формулировка)** | **Индикатор достижения компетенции**  **(код и формулировка)** | **Перечень**  **планируемых результатов обучения** |
| **Универсальные компетенции** | | |
| **УК-2**  Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений | ИД-УК-2.1  При разработке и реализации проектов выбирает способы решения задач исходя из действующих правовых норм. | Знать:   * правовые нормы в области информационной безопасности;   Уметь:   * выбирать способы решения профессиональных задач, исходя из действующих правовых норм в области информационной безопасности. |
| ИД-УК-2.2  Определяет круг задач в рамках поставленной цели и выбирает способы решения, исходя из имеющихся ресурсов и ограничений. | Уметь:   * определять задачи по соблюдению правовых ограничений в области информационной безопасности в ходе профессиональной деятельности.   Владеть навыками:   * самостоятельного поиска актуальных правовых ограничений, в рамках которых могут быть решены профессиональные задачи. |

**4. Объём, структура и содержание дисциплины**

Общая трудоёмкость дисциплины составляет **2** зачёт. ед., **72** акад. час.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Темы (разделы)**  **дисциплины,**  **их содержание** | **Семестр** | **Виды учебных занятий,**  **включая самостоятельную работу студентов,**  **и их трудоемкость**  **(в академических часах)** | | | | | | **Формы текущего контроля успеваемости**  **Форма промежуточной аттестации**  ***(по семестрам)*** |
| **Контактная работа** | | | | | самостоятельная  работа |
| лекции | практические | лабораторные | консультации | аттестационные испытания |
| 1 | Основные принципы правового регулирова-ния информационной безопасности | 8 | 2 |  |  | 0,25 |  | 4 | Реферат №1 |
| 2 | Правовое обеспечение информационной безопасности личности | 8 | 2 |  |  |  |  | 4 | Реферат №2 |
| 3 | Правовое обеспечение информационной безопасности государства | 8 | 2 |  |  | 0,25 |  | 4 |
| 4 | Правовое обеспечение информационной безопасности бизнеса | 8 | 2 |  |  | 0,25 |  | 4 |
| 5 | Правовое обеспечение информационной безопасности общества | 8 | 2 |  |  | 0,25 |  | 4 |
| 6 | Правовые средства обеспечения информационной безопасности | 8 | 2 |  |  | 0,25 |  | 4 | Реферат №3 |
| 7 | Правовое обеспечение информационной безопасности электронного документооборота | 8 | 2 |  |  | 0,25 |  | 4 |
| 8 | Правовое обеспечение безопасности информационной инфраструктуры | 8 | 2 |  |  | 0,25 |  | 4 |
| 9 | Проблемы правового закрепления принципов обеспечения междуна-родной информацион-ной безопасности | 8 | 1 |  |  | 0,25 |  | 4 |
|  | Промежуточная аттестация | 8 |  |  |  |  | 0,3 | 16,7 | Зачёт |
|  | **ИТОГО** | ***8*** | **17** |  |  | **2** | **0,3** | **52,7** | **72** |
|  | ***в том числе с ЭО и ДОТ*** |  |  |  |  |  |  |  |  |

**Содержание разделов дисциплины**

*Тема № 1*

***Основные принципы правового регулирования информационной безопасности***

Юридический смысл понятия «безопасность»: цели, объекты защиты, угрозы безопасности. Информационная безопасность в системе безопасности. Источники и содержание угроз интересам личности, общества и государства в информационной сфере.

Доктрина информационной безопасности Российской Федерации, направления ее развития. Стратегия национальной безопасности Российской Федерации до 2020 года и информационная безопасность. Стратегия развития информационного общества в Российской Федерации и информационная безопасность.

Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.

Методы обеспечения информационной безопасности (правовые, организационно-технические, экономические). Специальные режимы распространения информации. Структура нормативно-правовых актов в области обеспечения информационной безопасности. Правовые механизмы обеспечения безопасности объектов защиты: информации, прав на информацию, информационных систем, информационно-коммуникационной инфраструктуры. Принцип технологической нейтральности законодательных актов. Соотношение нормативно-правовых и нормативно-технических методов обеспечения безопасности объектов защиты.

Юридические права и обязанности субъектов обеспечения информационной безопасности: граждан, коммерческих и некоммерческих организаций, органов государственной власти и органов местного самоуправления.

*Тема № 2*

***Правовое обеспечение информационной безопасности личности***

Угрозы правам человека в информационной сфере.

"Информационная приватность" личности в информационном обществе: цели, возможности обеспечения, состояние правовой защиты. Персональные данные и режимы конфиденциальности.

Информационно-психологическая безопасность личности. Социальные сети и «подмена личности». Организационно-правовые меры защиты интересов личности при сборе данных о пользователях в сети Интернет.

Цифровые идентификаторы как юридические средства идентификации (аутентификации) личности.

*Тема № 3*

***Правовое обеспечение информационной безопасности государства***

Проблемы обеспечения информационной безопасности «Электронного государства»: правовое обеспечение информационного суверенитета России, информационная безопасность в системе государственной и муниципальной службы, организационно-правовые меры обеспечения безопасности открытых данных.

Информационная безопасность при предоставлении электронных государственных и муниципальных услуг. Информационная безопасность электронных выборов, электронного голосования.

Правовое регулирование импортозамещения в целях обеспечения информационной безопасности государства.

*Тема № 4*

***Правовое обеспечение информационной безопасности бизнеса***

Защита корпоративной информации. Правовые режимы корпоративной информации (общедоступная информация, информация ограниченного доступа) и организационно-технические средства защиты (ограничение доступа, шифрование). Защита права на доступ к информации, необходимой для ведения бизнеса. Право доступа и условия доступа к информации.

Требования по защите корпоративных компьютерных систем и сетей в специальных или отраслевых законах. Ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации (применение средств защиты информации, лицензирование отдельных видов деятельности по обеспечению информационной безопасности).

Ответственность за нарушение требований по обеспечению информационной безопасности бизнеса.

*Тема № 5*

***Правовое обеспечение информационной безопасности общества***

Правовые механизмы противодействия распространению в Интернете противоправной информации. Обязанности организатора распространения информации в сети "Интернет". Обязанности блогера. "Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет". Порядок ограничения доступа к информации, распространяемой с нарушением авторских и (или) смежных прав. Порядок ограничения доступа к информации, распространяемой с нарушением закона. Защита детей от информации, причиняющей вред их здоровью и развитию.

Культура информационной безопасности как необходимый регулятор в информационном обществе.

Проблемы сохранения культурного наследия, созданного в электронном виде.

Проекты «Безопасный город».

*Тема № 6*

***Правовые средства обеспечения информационной безопасности***

Лицензирование деятельности, связанной с защитой информации. Сертификация средств защиты информации. Аккредитация и аттестация в сфере обеспечения информационной безопасности.

Требования к организации защиты информации.

Отечественные и международные стандарты в области информационной безопасности.

*Тема № 7*

***Правовое обеспечение информационной безопасности электронного документооборота***

Юридически значимый защищенный электронный документооборот: требования и средства обеспечения.

Правовое регулирование применения криптографических средств защиты информации и средств электронной подписи. Проблемы идентификации и аутентификации участников электронного документооборота, в том числе при получении государственных и муниципальных услуг в электронном виде.

Проблемы архивного хранения информации в электронной форме.

*Тема № 8*

***Правовое обеспечение безопасности информационной инфраструктуры***

Государственные информационные системы. Реестр федеральных государственных информационных систем. Муниципальные информационные системы, созданные на основании решения органа местного самоуправления. Единая система идентификации и аутентификации, порядок использования единой системы идентификации и аутентификации.

Обеспечение безопасности при создании информационных систем, их эксплуатации и защите содержащейся в них информации.

Законодательное регулирование создания и функционирования отдельных государственных информационных систем (ГАС «Выборы», ГИС ЖКХ, ГАИС «ЭРА-ГЛОНАС», ГИС ТЭК).

Правовые средства обеспечения безопасности сетей связи. Правовые проблемы обеспечения информационной безопасности в условиях трансграничности информационно-коммуникационных сетей. Ответственность за нарушение требований по защите информационных систем. Правовые последствия анонимности подключения к Интернету. Правовые проблемы обеспечения ответственности за правонарушения в сфере информационной безопасности: а) уголовная ответственность за правонарушения в сфере информационной безопасности, тенденции развития уголовного права применительно к преступлениям с использованием интернета; б) административная ответственность за правонарушения в сфере информационной безопасности; в) гражданско-правовая ответственность за правонарушения в сфере информационной безопасности.

*Тема № 9*

***Проблемы правового закрепления принципов обеспечения международной информационной безопасности***

Международная информационная безопасность и кибербезопасность. Проблемы развития международного гуманитарного права применительно к угрозам в информационной сфере.

Региональные стратегии обеспечения коллективной информационной безопасности.

Инициативы Российской Федерации в сфере обеспечения международной информационной безопасности.

**5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине**

В процессе обучения проводятся лекционные занятия, в ходе которых используются следующие типы занятий и образовательные технологии.

**Вводная лекция** – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

**Академическая лекция** (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

**Консультация** – занятие, посвящённое консультациям по организации самостоятельной работы, ответам на вопросы студентов или разбору трудных тем.

Электронное обучение и дистанционные образовательные технологии используются только во время действия приказа о переходе на смешанное очно-дистанционное обучение в объёме материалов э**лектронного учебного курса «Правовые основы информационной безопасности» в LMS Электронный университет Moodle ЯрГУ**, в котором:

* представлены правила прохождения промежуточной аттестации по дисциплине;
* представлен список учебной литературы, рекомендуемой для освоения дисциплины;
* представлена информация о форме и времени проведения консультаций по дисциплине в режиме онлайн;
* посредством форума осуществляется синхронное и (или) асинхронное взаимодействие между обучающимися и преподавателем в рамках изучения дисциплины.

**6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине**

В процессе осуществления образовательного процесса по дисциплине используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;

- Adobe Acrobat Reader.

**7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)**

В процессе осуществления образовательного процесса по дисциплине используются:

**а) профессиональные базы данных:**

1. Автоматизированная библиотечно-информационная система «БУКИ-NEXT»: <http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php>
2. Портал научной электронной библиотеки: http://elibrary.ru/defaultx.asp
3. Федеральная университетская компьютерная сеть России: http://www.runnet.ru/
4. Единый портал для размещения информации о разработке федеральными органами исполнительной власти проектов нормативных правовых актов и результатов их общественного обсуждения: <http://regulation.gov.ru/>

**б) информационные справочные правовые системы:**

1. СПС «Консультант-плюс»: http://www.consultant.ru/
2. СПС «Гарант»: http://www.garant.ru/

**8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины**

а) основная литература:

1. Мельников В. П. Информационная безопасность и защита информации: учеб. пособие для вузов. / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - М.: Академия, 2006. - 331 с.
2. Новиков, В. К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) : учебное пособие [Электронный ресурс] / В. К. Новиков. - Москва : Горячая линия - Телеком, 2015. - 176 с. URL: <https://www.studentlibrary.ru/book/ISBN9785991205252.html>

б) дополнительная литература:

1. Борисов М. А., Романов О. А. Основы организационно-правовой защиты информации: [учеб. пособие для вузов.]. - 2-е изд. - М.: URSS; ЛИБРОКОМ, 2013. - 203 с.
2. Серго, А. Г. Основы права интеллектуальной собственности [Электронный ресурс] / Серго А. Г. , Пущин В. С. - Москва : НОУ "ИНТУИТ", 2016. URL: <https://www.studentlibrary.ru/book/ISBN5955600477.html>

в) ресурсы сети «Интернет»

1. Электронная библиотека учебных материалов ЯрГУ (http://www.lib.uniyar.ac.ru/opac/bk\_cat\_find.php).
2. Официальный сайт Президента Российской Федерации: <http://kremlin.ru/>
3. Официальный сайт Государственной Думы (АСОЗД): http://www.duma.gov.ru/; <http://asozd2.duma.gov.ru/>
4. Официальный сайт Совета Федерации: <http://www.council.gov.ru/>
5. Официальный сайт Правительства Российской Федерации: http://government.ru/
6. Сайт Совета Безопасности Российской Федерации: http://www.scrf.gov.ru/security/information/
7. Сайт ФСТЭК России: https://fstec.ru/
8. Сайт ФСБ России: <http://www.fsb.ru/>
9. Сайт Минкомсвязи России: <http://minsvyaz.ru/>
10. Единый портал для размещения информации о разработке федеральными органами исполнительной власти проектов нормативных правовых актов и результатов их общественного обсуждения: <http://regulation.gov.ru/>

**9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине**

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

* учебные аудитории для проведения занятий лекционного типа;
* учебные аудитории для проведения групповых и индивидуальных консультаций,
* учебные аудитории для проведения текущего контроля и промежуточной аттестации;
* помещения для самостоятельной работы;
* помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока.

Автор:

Доцент кафедры

интеллектуальных информационных

радиофизических систем, к. ф.-м. н. Т. К. Артёмова

**Приложение № 1 к рабочей программе дисциплины**

**«Правовые основы информационной безопасности»**

**Фонд оценочных средств**

**для проведения текущего контроля успеваемости**

**и промежуточной аттестации студентов**

**по дисциплине**

1. **Типовые контрольные задания и иные материалы,**

**используемые в процессе текущего контроля успеваемости**

**Темы рефератов**

(рефераты представляются в виде документа, а также в форме доклада по материалу реферата, длительность доклада – 7 минут)

**По 1 разделу – реферат №1**

1. Угрозы интересам личности, общества и государства в информационной сфере.
2. Основные положения доктрины информационной безопасности Российской Федерации, стратегии национальной безопасности Российской Федерации, стратегии развития информационного общества в Российской Федерации.
3. Организационно-технические методы обеспечения информационной безопасности.
4. Специальные режимы распространения информации.
5. Реализация принципа технологической нейтральности законодательных актов в российском законодательстве.

**По темам 2 – 5 – реферат №2**

1. Цифровые идентификаторы как юридические средства идентификации (аутентификации) личности.
2. Информационная безопасность при предоставлении электронных государственных и муниципальных услуг.
3. Информационная безопасность электронных выборов, электронного голосования.
4. Организационно-технические средства защиты корпоративной информации.
5. Требования по защите корпоративных компьютерных систем и сетей в специальных или отраслевых законах.
6. Культура информационной безопасности как необходимый регулятор в информационном обществе.
7. Проблемы сохранения культурного наследия, созданного в электронном виде.
8. Проекты «Безопасный город».

**По темам 6 – 9 – реферат №3**

1. Сертификация средств защиты информации. Аккредитация и аттестация в сфере обеспечения информационной безопасности.
2. Правовое регулирование применения криптографических средств защиты информации и средств электронной подписи.
3. Проблемы идентификации и аутентификации участников электронного документооборота, в том числе при получении государственных и муниципальных услуг в электронном виде.
4. Проблемы архивного хранения информации в электронной форме.
5. Единая система идентификации и аутентификации, порядок использования единой системы идентификации и аутентификации.
6. Законодательное регулирование создания и функционирования отдельных государственных информационных систем (ГАС «Выборы», ГИС ЖКХ, ГАИС «ЭРА-ГЛОНАС», ГИС ТЭК).
7. Инициативы Российской Федерации в сфере обеспечения международной информационной безопасности.

**Критерии оценивания реферата**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Критерий** | **Пороговый уровень** | | **Повышенный уровень** | | **Высокий уровень** | |
| значение | баллы | значение | баллы | значение | баллы |
| Объём реферата | до 2-х страниц содержательного текста | 1 | 3-4 страницы содержательного текста | 2 | более 4-х страниц содержательного текста | 3 |
| Количество источников | до 2-х | 1 | 3-5 | 2 | более 5 | 3 |
| Содержание соответствует теме | частично | 2 | в целом соответствует | 4 | полностью | 6 |
| Приведены положения нормативных документов | не приведены, только названы нормативные документы | 2 | приведены, но не все | 4 | полностью приведены | 6 |
| Приведены примеры из практики правоприменения | на 1-2 положения | 2 | к половине положений | 4 | ко всем или почти всем положениям | 6 |
| Оформление | есть, текст читабельный | 1 | близкое к ГОСТ | 2 | по ГОСТ «Отчёт о НИР» | 3 |

Реферат оценивается пороговым уровнем, если набрано 6-9 баллов, повышенным – 10-18 баллов, высоким – более 18 баллов.

**2 Список вопросов и (или) заданий для проведения промежуточной аттестации**

**Список вопросов к зачёту**

(зачёт выставляется по результатам рефератов и ответов на вопросы)

1. Юридический смысл понятия «безопасность»: цели, объекты защиты, угрозы безопасности. Информационная безопасность в системе безопасности.
2. Источники и содержание угроз интересам личности, общества и государства в информационной сфере.
3. Доктрина информационной безопасности Российской Федерации, направления ее развития. Стратегия национальной безопасности Российской Федерации до 2020 года и информационная безопасность. Стратегия развития информационного общества в Российской Федерации и информационная безопасность.
4. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.
5. Методы обеспечения информационной безопасности (правовые, организационно-технические, экономические).
6. Специальные режимы распространения информации.
7. Структура нормативно-правовых актов в области обеспечения информационной безопасности.
8. Правовые механизмы обеспечения безопасности объектов защиты: информации, прав на информацию, информационных систем, информационно-коммуникационной инфраструктуры.
9. Принцип технологической нейтральности законодательных актов.
10. Соотношение нормативно-правовых и нормативно-технических методов обеспечения безопасности объектов защиты.
11. Юридические права и обязанности субъектов обеспечения информационной безопасности: граждан, коммерческих и некоммерческих организаций, органов государственной власти и органов местного самоуправления.
12. Угрозы правам человека в информационной сфере.
13. "Информационная приватность" личности в информационном обществе: цели, возможности обеспечения, состояние правовой защиты. Персональные данные и режимы конфиденциальности.
14. Информационно-психологическая безопасность личности. Социальные сети и «подмена личности». Организационно-правовые меры защиты интересов личности при сборе данных о пользователях в сети Интернет.
15. Цифровые идентификаторы как юридические средства идентификации (аутентификации) личности.
16. Проблемы обеспечения информационной безопасности «Электронного государства»: правовое обеспечение информационного суверенитета России, информационная безопасность в системе государственной и муниципальной службы, организационно-правовые меры обеспечения безопасности открытых данных.
17. Информационная безопасность при предоставлении электронных государственных и муниципальных услуг.
18. Информационная безопасность электронных выборов, электронного голосования.
19. Правовое регулирование импортозамещения в целях обеспечения информационной безопасности государства.
20. Защита корпоративной информации. Правовые режимы корпоративной информации (общедоступная информация, информация ограниченного доступа) и организационно-технические средства защиты (ограничение доступа, шифрование).
21. Защита права на доступ к информации, необходимой для ведения бизнеса. Право доступа и условия доступа к информации.
22. Требования по защите корпоративных компьютерных систем и сетей в специальных или отраслевых законах.
23. Ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации (применение средств защиты информации, лицензирование отдельных видов деятельности по обеспечению информационной безопасности).
24. Ответственность за нарушение требований по обеспечению информационной безопасности бизнеса.
25. Правовые механизмы противодействия распространению в Интернете противоправной информации. Обязанности организатора распространения информации в сети "Интернет". Обязанности блогера. "Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет". Порядок ограничения доступа к информации, распространяемой с нарушением авторских и (или) смежных прав. Порядок ограничения доступа к информации, распространяемой с нарушением закона. Защита детей от информации, причиняющей вред их здоровью и развитию.
26. Культура информационной безопасности как необходимый регулятор в информационном обществе.
27. Проблемы сохранения культурного наследия, созданного в электронном виде.
28. Проекты «Безопасный город».
29. Лицензирование деятельности, связанной с защитой информации.
30. Сертификация средств защиты информации.
31. Требования к организации защиты информации.
32. Аккредитация и аттестация в сфере обеспечения информационной безопасности.
33. Отечественные и международные стандарты в области информационной безопасности.
34. Юридически значимый защищенный электронный документооборот: требования и средства обеспечения.
35. Правовое регулирование применения криптографических средств защиты информации и средств электронной подписи.
36. Проблемы идентификации и аутентификации участников электронного документооборота, в том числе при получении государственных и муниципальных услуг в электронном виде.
37. Проблемы архивного хранения информации в электронной форме.
38. Государственные информационные системы. Реестр федеральных государственных информационных систем. Муниципальные информационные системы, созданные на основании решения органа местного самоуправления.
39. Единая система идентификации и аутентификации, порядок использования единой системы идентификации и аутентификации.
40. Обеспечение безопасности при создании информационных систем, их эксплуатации и защите содержащейся в них информации.
41. Законодательное регулирование создания и функционирования отдельных государственных информационных систем (ГАС «Выборы», ГИС ЖКХ, ГАИС «ЭРА-ГЛОНАС», ГИС ТЭК).
42. Ответственность за нарушение требований по защите информационных систем. Правовые последствия анонимности подключения к Интернету.
43. Правовые средства обеспечения безопасности сетей связи. Правовые проблемы обеспечения информационной безопасности в условиях трансграничности информационно-коммуникационных сетей.
44. Правовые проблемы обеспечения ответственности за правонарушения в сфере информационной безопасности: а) уголовная ответственность за правонарушения в сфере информационной безопасности, тенденции развития уголовного права применительно к преступлениям с использованием интернета; б) административная ответственность за правонарушения в сфере информационной безопасности; в) гражданско-правовая ответственность за правонарушения в сфере информационной безопасности.
45. Международная информационная безопасность и кибербезопасность.
46. Проблемы развития международного гуманитарного права применительно к угрозам в информационной сфере.
47. Региональные стратегии обеспечения коллективной информационной безопасности.
48. Инициативы Российской Федерации в сфере обеспечения международной информационной безопасности.

**Критерии оценивания ответа на вопрос билета**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Критерий** | **Пороговый уровень** | | **Повышенный уровень** | | **Высокий уровень** | |
| значение | баллы | значение | баллы | значение | баллы |
| Полнота раскрытия темы | изложено 25-50% | 1 | большая часть | 2 | полностью или почти полностью | 3 |
| Приведены положения нормативных документов | не приведены, только названы нормативные документы | 1 | приведены, но не все | 2 | полностью или почти полностью приведены | 3 |
| Приведены примеры из практики правоприменения | на 1-2 положения | 1 | к половине положений | 2 | ко всем или почти всем положениям | 3 |

Ответ на вопрос оценивается пороговым уровнем, если набрано 2-3 балла, повышенным – 4-6 баллов, высоким – более 6 баллов.

**Правила выставления оценки за зачёт**

Оценка складывается из оценки за рефераты и ответы на вопросы билета на зачёте (3 вопроса, 1 – по теме 1, 2-ой – по темам 2 – 5, 3-ий – по темам 6 – 9). См. ниже таблицу общих требований и критерии оценивания по компонентам.

|  |  |  |
| --- | --- | --- |
| На «Зачтено» | На «Зачтено», продвинутый уровень | На «Зачтено», высокий уровень |
| 1. Ответ на вопрос билета не хуже 2-х из 9 баллов.  2. Рефераты 2, 3 сданы, оценка не ниже 6 баллов | 1. Ответ на вопрос билета 3-6 из 9 баллов.  2. Рефераты 2, 3 выполнены с небольшими недостатками (оценка 10-18 баллов). | 1. Ответ на вопрос билета не хуже 7 из 9 баллов.  2. Рефераты 2, 3 выполнены отлично, с примерами и аргументами (оценка более 18 баллов). |

Если критерии на «зачтено» не выполнены, выставляется оценка «не зачтено».

**Приложение № 2 к рабочей программе дисциплины**

**«Правовые основы информационной безопасности»**

**Методические указания для студентов по освоению дисциплины**

Основной формой занятий по дисциплине являются лекции, на которых излагаются теоретические основы, методы, принципы.

Для успешного освоения дисциплины обязательно чтение нормативной и правовой документации, составляющей основную долю литературы по тематике курса.

Для успешного освоения дисциплины обязательно также выполнение рефератов 1, 2, 3. Реферат должен оформляться в соответствии с ГОСТ «Отчёт о НИР», ГОСТ «Ссылка библиографическая» и должен содержать: постановку проблематики, обзор законодательства, обзор правоприменительной практики, собственные выводы и аргументы в пользу этих выводов.

Изучение дисциплины заканчивается зачётом.

Оценка за зачёт складывается из оценки за рефераты и ответы на вопросы на зачёте (3 вопроса, 1 – по теме 1, 2-ой – по темам 2 – 5, 3-ий – по темам 6 – 9). См. ниже таблицу общих требований и критерии оценивания по компонентам.

|  |  |  |
| --- | --- | --- |
| На «Зачтено» | На «Зачтено», продвинутый уровень | На «Зачтено», высокий уровень |
| 1. Ответ на вопрос зачёта не хуже 2-х из 9 баллов.  2. Рефераты 2, 3 сданы, оценка не ниже 6 баллов | 1. Ответ на вопрос зачёта 3-6 из 9 баллов.  2. Рефераты 2, 3 выполнены с небольшими недостатками (оценка 10-18 баллов). | 1. Ответ на вопрос зачёта ну хуже 7 из 9 баллов.  2. Рефераты 2, 3 выполнены отлично, с примерами и аргументами (оценка более 18 баллов). |

**Критерии оценивания ответа на вопрос билета**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Критерий** | **Пороговый уровень** | | **Повышенный уровень** | | **Высокий уровень** | |
| значение | баллы | значение | баллы | значение | баллы |
| Полнота раскрытия темы | изложено 25-50% | 1 | большая часть | 2 | полностью или почти полностью | 3 |
| Приведены положения нормативных документов | не приведены, только названы нормативные документы | 1 | приведены, но не все | 2 | полностью или почти полностью приведены | 3 |
| Приведены примеры из практики правоприменения | на 1-2 положения | 1 | к половине положений | 2 | ко всем или почти всем положениям | 3 |

Ответ на вопрос оценивается пороговым уровнем, если набрано 2-3 балла, повышенным – 4-6 баллов, высоким – более 6 баллов.

**Критерии оценивания реферата**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Критерий** | **Пороговый уровень** | | **Повышенный уровень** | | **Высокий уровень** | |
| значение | баллы | значение | баллы | значение | баллы |
| Объём реферата | до 2-х страниц содержательного текста | 1 | 3-4 страницы содержательного текста | 2 | более 4-х страниц содержательного текста | 3 |
| Количество источников | до 2-х | 1 | 3-5 | 2 | более 5 | 3 |
| Содержание соответствует теме | частично | 2 | в целом соответствует | 4 | полностью | 6 |
| Приведены положения нормативных документов | не приведены, только названы нормативные документы | 2 | приведены, но не все | 4 | полностью приведены | 6 |
| Приведены примеры из практики правоприменения | на 1-2 положения | 2 | к половине положений | 4 | ко всем или почти всем положениям | 6 |
| Оформление | есть, текст читабельный | 1 | близкое к ГОСТ | 2 | по ГОСТ «Отчёт о НИР» | 3 |

Реферат оценивается пороговым уровнем, если набрано 6-9 баллов, повышенным – 10-18 баллов, высоким – более 18 баллов.

**Учебно-методическое обеспечение**

**самостоятельной работы студентов по дисциплине**

**1. Для самостоятельной работы** рекомендуется использовать учебную литературу, указанную в рабочей программе, а также ресурсы Интернет, предоставляющие доступ к нормативным, регламентирующим и другим официальным документам.

Для самостоятельного подбора литературы в библиотеке ЯрГУ рекомендуется использовать:

**1. Личный кабинет** (<http://lib.uniyar.ac.ru/opac/bk_login.php>) дает возможность получения on-line доступа к списку выданной в автоматизированном режиме литературы, просмотра и копирования электронных версий изданий сотрудников университета (учеб. и метод. пособия, тексты лекций и т.д.) Для работы в «Личном кабинете» необходимо зайти на сайт Научной библиотеки ЯрГУ с любой точки, имеющей доступ в Internet, в пункт меню «Электронный каталог»; пройти процедуру авторизации, выбрав вкладку «Авторизация», и заполнить представленные поля информации.

**2. Электронная библиотека учебных материалов ЯрГУ**

(<http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php>) содержит более 2500 полных текстов учебных и учебно-методических материалов по основным изучаемым дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/паролю.

**3. Электронная картотека** [**«Книгообеспеченность»**](http://10.1.0.4/buki/bk_bookreq_find.php)

(<http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php>) раскрывает учебный фонд научной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии книгообеспеченности дисциплин основной и дополнительной литературой, а также цикла дисциплин и специальностей. Электронная картотека [«Книгообеспеченность»](http://10.1.0.4/buki/bk_bookreq_find.php) доступна в сети университета и через Личный кабинет.

**4. Электронно-библиотечные системы**, доступ к которым осуществляется через подписку ЯрГУ (<http://www.lib.uniyar.ac.ru/content/resource/net_res(1).php> ).