МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__8__» ___08___ 2023 г.

Нормативно-правовое регулирование в сфере информационной безопасности

Методические указания по организации самостоятельной работы по дисциплине «Нормативно-правовое регулирование в сфере информационной безопасности» для студентов направления подготовки 10.04.01 «Информационная безопасность»

Курск 2023

УДК 004.773.5

Составители: Кулешова Е.А.

Рецензент

Кандидат технических наук, доцент кафедры
вычислительной техники А.В. Киселев

Нормативно-правовое регулирование в сфере информационной безопасности: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 27 с.: Библиогр.: с. 27.

Содержат сведения по вопросам самостоятельной работы на протяжении изучения дисциплины. Указывается порядок выполнения самостоятельных работ, содержание работы.

Предназначены для студентов направления подготовки 10.04.01 «Информационная безопасность».

Текст печатается в авторской редакции
Подписано в печать . Формат 60x84 1/16.
Усл. печ.л. . Уч. –изд.л. .Тираж 50 экз. Заказ .
Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Самостоятельная работа № 1 -

Информация, информационные системы как объект правового регулирования информационной безопасности

Закон РФ «О государственной тайне» регулирует отношения, возникающие в связи с отношением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности РФ.

В качестве базы для Закона «О государственной тайне» был избран Закон РФ «О безопасности» от 28 декабря 2010 г., впервые введенный в действие Постановлением Верховного Совета РФ 05.03.1992 г.

Порядок засекречивания сведений и их носителей определяет 3 раздел закона «О государственной тайне». В ней представлены:

→ принципы засекречивания;

→ сведения, не подлежащие засекречиванию;

→ степени секретности сведений и грифы секретности носителей этих сведений;

→ порядок отнесения сведений к государственной тайне;

→ ограничение прав собственности предприятий, учреждений, организаций и граждан РФ на информацию в связи с ее засекречиванием;

→ порядок засекречивания сведений и их носителей;

→ реквизиты носителей сведений, составляющих государственную тайну.

В четвертом разделе дан порядок рассекречивания сведений и их носителей, включающий:

→ порядок рассекречивания сведений;

→ порядок рассекречивания носителей сведений, составляющих государственную тайну;

→ порядок исполнения запросов граждан, предприятий, учреждений, организаций и органов государственной власти РФ о рассекречивании сведений.

Задание: Исследовательский проект

Цель проекта: Изучить и проанализировать правовое регулирование информационной безопасности в отношении информации и информационных систем.

Шаги проекта:

1. Составьте обзор литературы о правовом регулировании информационной безопасности, особенно в отношении информации и информационных систем.
2. Изучите ключевые законы и нормативные акты, регулирующие информационную безопасность, включая международные и национальные нормы.
3. Сравните и проанализируйте различные подходы к правовому регулированию информационной безопасности в разных странах.
4. Исследуйте судебную практику и прецеденты, связанные с нарушениями информационной безопасности и соответствующими правовыми последствиями.
5. Проведите анализ действующего законодательства на предмет его эффективности и соответствия современным вызовам информационной безопасности.
6. Выполните сравнительный анализ стандартов и рекомендаций по информационной безопасности, которые применяются в различных отраслях и организациях.
7. Проанализируйте механизмы обеспечения соблюдения правил и требований информационной безопасности, включая контроль, наказания и ответственность.
8. Сделайте выводы о сильных и слабых сторонах существующего правового регулирования информационной безопасности и предложите возможные улучшения.

Ожидаемые результаты проекта:

- Обзор литературы по правовому регулированию информационной безопасности.

- Анализ действующего законодательства и его соответствия современным вызовам информационной безопасности.
- Сравнительный анализ стандартов и рекомендаций по информационной безопасности.
- Выводы о сильных и слабых сторонах существующего правового регулирования и предложения по его улучшению.

Вопросы:

1. Порядок разработки перечня сведений, подлежащих засекречиванию.
2. Процедура предварительного засекречивания.
3. Порядок рассекречивания.
4. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию.
5. Какое понятие имеет информация в контексте правового регулирования информационной безопасности?
6. Какие основные законы и нормативные акты регулируют информационную безопасность?
7. Какие права и обязанности пользователей информационных систем установлены законодательством?
8. Что такое персональные данные и как они защищаются согласно законодательству?
9. Какое значение имеет интеллектуальная собственность в контексте информационной безопасности?
10. Какие меры предусмотрены для защиты государственной информации от несанкционированного доступа?
11. Какие ответственность и наказания предусмотрены за нарушение правил информационной безопасности?
12. Какие требования к безопасности информационных систем установлены законодательством?
13. Какие меры принимаются для защиты коммерческой и конфиденциальной информации?
14. Какие меры предусмотрены для защиты личных данных пользователей при использовании онлайн-сервисов?

15. Какие международные соглашения и стандарты существуют в области информационной безопасности и их правовое значение?

Самостоятельная работа №2 -
Правовая основа допуска и доступа персонала к защищаемым сведениям.

СВЕДЕНИЯ, ОТНОСИМЫЕ К ГТ			
Сведения в военной области	Сведения в области экономики науки, техники	Сведения В области внешней политики и экономики	Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности

Классификация сведений, относимых к государственной тайне

Важной особенностью настоящей концепции защиты информации является переход от принципа «интегральной защиты» информации к «дифференциальной защите», обеспечивающей разумную достаточность в соответствии с запросами государственных структур и отдельных граждан. При этом необходимо отметить, что все законодательные акты имеют содержательную различную направленность по защите информации в органах государственной власти и частных лиц. Задача создания стройной законодательной системы, одновременно удовлетворяющей всем изложенным требованиям комплексной защиты информации, оказывается сложной задачей и на сегодняшний день не имеет адекватных решений.

Определяющим принципом конституционных информационных отношений является принцип свободы и ограничения информации. Принцип свободы в более широком контексте является центральным принципом всего конституционного регулирования. Конституция официально подтверждает международно-признанное право граждан на информацию. Статьи Конституции РФ раскрывают содержание этого права. Пункт 4 ст. 29 гласит: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом».

Задание: Исследование правовой основы допуска и доступа персонала к защищаемым сведениям

1. Введение

Определите понятие "защищаемые сведения" и объясните их значение в контексте безопасности информации.

2. Анализ законодательства

Изучите соответствующие нормативные акты, регулирующие допуск и доступ персонала к защищаемым сведениям.

Сделайте обзор основных законов, указов, постановлений или других документов, определяющих требования к допуску и доступу персонала.

3. Права и обязанности персонала

Разработайте список прав и обязанностей, которые должны выполнять сотрудники при работе с защищаемыми сведениями.

Проанализируйте, какие меры безопасности требуются от персонала для обеспечения конфиденциальности и целостности защищаемых сведений.

4. Процедуры допуска и доступа

Изучите процедуры допуска персонала к защищаемым сведениям (например, проверка удостоверений личности, прохождение курсов обучения и т. д.).

Опишите процедуры доступа персонала к защищаемым сведениям (например, использование уникальных идентификаторов, двухфакторной аутентификации и т. д.).

5. Контроль и наказание

Изучите механизмы контроля и наказания в случае нарушения правил допуска и доступа персонала к защищаемым сведениям.

Рассмотрите примеры санкций, которые могут быть применены при нарушении безопасности информации со стороны персонала.

6. Заключение

Подведите итоги исследования и сформулируйте ключевые выводы о правовой основе допуска и доступа персонала к защищаемым сведениям.

Вопросы:

1. В каком порядке информация относится к Государственной тайне?
2. Какими законами и актами раскрывается право граждан на информацию?
3. В каком разделе закона «О государственной тайне» определен порядок распоряжения сведениями, составляющими государственную тайну?
4. Какие законы и нормативные акты устанавливают правила и требования к допуску и доступу персонала к защищаемым сведениям?
5. Какие виды классификации информации используются для определения уровня доступа персонала?
6. Какие процедуры предусмотрены для получения допуска к защищаемым сведениям?
7. Какие требования предъявляются к персоналу, желающему получить допуск к защищаемым сведениям?
8. Какие ограничения могут быть наложены на допуск и доступ персонала к защищаемым сведениям в соответствии с законодательством?
9. Каким образом проверяется достоверность предоставленной персоналом информации при процессе допуска?
10. Какие полномочия и ответственность имеют лица, ответственные за предоставление и контроль допуска персонала к защищаемым сведениям?
11. Какие меры безопасности принимаются для защиты защищаемых сведений от несанкционированного доступа со стороны персонала?
12. Какие права имеет персонал в отношении доступа к защищаемым сведениям и как они регулируются законодательством?
13. Какие меры предусмотрены для обучения персонала в области безопасности информации и защиты защищаемых сведений?

14. Какие виды контроля осуществляются для проверки соблюдения правил и требований при доступе персонала к защищаемым сведениям?

15. Какие наказания предусмотрены за нарушение правил допуска и доступа персонала к защищаемым сведениям?

Самостоятельная работа №3-

Правовые основы защиты коммерческой тайны.

Основным условием обеспечения сохранности коммерческой тайны является персональная ответственность должностных лиц фирмы всех уровней и других ее работников, которым предоставлен доступ к коммерческой тайне, за соблюдение режима конфиденциальности, установленного упомянутыми организационно-методическими документами (доводятся до сведения указанных лиц под расписку). Должностные лица и сотрудники организации (фирмы) в случае разглашения ими информации, составляющей предмет защиты конфиденциальных интересов, нарушения порядка обращения с материальными носителями конфиденциальной информации или средствами информатизации и связи, используемыми для обработки и передачи указанной информации, а также в случае несанкционированного ознакомления с объектами интеллектуальной собственности посторонних лиц, несут дисциплинарную и материальную ответственность.

Обязанность возмещения убытков от указанных неправомерных действий виновным лицом возникает в случае, если условия о соблюдении конфиденциальности включены в трудовой договор (контракт) с работником или гражданско-правовой договор с контрагентом (п. 2 ст.139 Гражданского кодекса). В случае деловых контактов фирмы с иностранными партнерами взаимные обязательства сторон о неразглашении информации, которая определяется ими как конфиденциальная, срок действия этих обязательств, санкции за их невыполнение и другие аспекты отражаются в рамках документа о намерениях сторон.

Передача конфиденциальной информации и объектов интеллектуальной собственности другим физическим и юридическим лицам производится на основе лицензионного договора.

Задание

Напишите реферат на тему "Правовые основы защиты коммерческой тайны", включающий следующие аспекты:

1. Определение коммерческой тайны и ее значение для успешного функционирования предприятий.
2. Правовые нормы, регулирующие защиту коммерческой тайны в вашей стране (можете выбрать свою страну или любую другую).
3. Виды информации, которые могут быть признаны коммерческой тайной.
4. Процедуры и меры, применяемые для защиты коммерческой тайны, включая конфиденциальность, неразглашение информации и контроль доступа.
5. Методы правового преследования нарушителей коммерческой тайны и возможные санкции.
6. Значение международных соглашений и организаций в области защиты коммерческой тайны.

В реферате необходимо использовать актуальные законодательные акты, примеры из судебной практики и научные исследования по данной теме. Обратите внимание на структуру работы, логическую последовательность аргументов и правильное оформление ссылок и источников информации.

Вопросы:

1. Что понимается под коммерческой тайной?
2. Какое значение имеет защита коммерческой тайны для предприятий?
3. Какие правовые нормы регулируют защиту коммерческой тайны в вашей стране?
4. Какие виды информации могут быть признаны коммерческой тайной?
5. Какие процедуры и меры применяются для защиты коммерческой тайны?
6. Какая роль у конфиденциальности в защите коммерческой тайны?

7. Как осуществляется контроль доступа к коммерческой тайне на предприятии?
8. Какие меры обеспечения безопасности информации используются для защиты коммерческой тайны?
9. Какие санкции предусмотрены для лиц, нарушающих коммерческую тайну?
10. Какие правовые способы пресечения нарушений коммерческой тайны существуют?
11. Какие международные соглашения и организации занимаются вопросами защиты коммерческой тайны?
12. Какие условия и требования необходимо соблюдать для признания информации коммерческой тайной?
13. Каковы основные различия между нарушением авторских прав и нарушением коммерческой тайны?
14. Какие риски несет предприятие, если коммерческая тайна была нарушена?
15. Какие примеры из практики судебных разбирательств свидетельствуют о важности защиты коммерческой тайны?

Самостоятельная работа №4 -

Компьютерная информация – как объект информатизации

Компьютерная информация - это набор данных, фактов и знаний, представленных в цифровой форме и хранящихся на компьютерных устройствах. Она может быть создана, обработана, передана и использована с использованием компьютерных систем и программного обеспечения.

Объект информатизации - это понятие, описывающее состояние или процесс превращения различных объектов и явлений в объекты, доступные для обработки, анализа и использования с использованием информационных технологий. Компьютерная информация является одним из таких объектов информатизации.

Под информатизацией понимается процесс внедрения и использования информационно-коммуникационных технологий (ИКТ) для обработки, передачи и хранения информации. Компьютерная информация становится объектом информатизации, когда она подвергается обработке, анализу или использованию с использованием компьютерных систем и технологий.

Раскрывая определение "компьютерной информации как объекта информатизации", можно сказать, что компьютерная информация становится доступной для автоматизированной обработки и использования с помощью компьютерных технологий. Таким образом, информатизация позволяет улучшить эффективность и точность работы с компьютерной информацией, ускоряет процессы принятия решений, оптимизирует использование ресурсов и обеспечивает более удобный доступ к информации.

15

Задание

Напишите реферат на тему "Компьютерная информация – как объект информатизации", включающий следующие аспекты:

1. Определение компьютерной информации и ее роль в современном обществе.
2. Развитие информационных технологий и их влияние на создание, хранение и передачу компьютерной информации.
3. Виды компьютерной информации: структурированная и неструктурированная информация, данные, программы, файлы и прочее.
4. Технологии информатизации и их применение для работы с компьютерной информацией (базы данных, информационные системы, облачные технологии и др.).
5. Проблемы безопасности компьютерной информации, включая угрозы, связанные с хранением, передачей и использованием данных.
6. Правовые и этические аспекты работы с компьютерной информацией, включая авторские права, защиту персональных данных и международные нормы.

В реферате необходимо использовать актуальные источники информации, научные статьи, законодательные акты и примеры из современной практики. Обратите внимание на структуру работы, логическую последовательность аргументов и правильное оформление ссылок и источников информации.

Вопросы

1. Что понимается под компьютерной информацией?
2. Какую роль компьютерная информация играет в современном обществе?
3. Какие технологии информатизации используются для работы с компьютерной информацией?
4. Какие виды компьютерной информации можно выделить?
5. Какие проблемы безопасности возникают при работе с компьютерной информацией?

6. Какие угрозы связаны с хранением компьютерной информации?
7. Какие меры безопасности следует принимать для защиты компьютерной информации?
8. Какие правовые и этические аспекты существуют при работе с компьютерной информацией?
9. Какие требования предъявляются к хранению и передаче персональных данных в контексте компьютерной информации?
10. Какие риски связаны с использованием облачных технологий для хранения компьютерной информации?
11. Какие основные принципы управления базами данных в контексте информатизации компьютерной информации?
12. Какие меры предусмотрены для обеспечения целостности и конфиденциальности компьютерной информации?
13. Какое значение имеют авторские права при работе с программными продуктами и компьютерной информацией?
14. Какие международные нормы регулируют работу с компьютерной информацией?
15. Какие последствия могут возникнуть при нарушении законодательства о компьютерной информации?

Самостоятельная работа №5 -
Лицензирование в области защиты информации.

Задание 1: Лицензирование в области защиты информации

Тема: Процедура получения лицензии на предоставление услуг по защите информации.

Описание задания:

Представьте себя в роли специалиста по защите информации, который хочет получить лицензию на предоставление услуг по защите информации. Ваше задание состоит в том, чтобы разработать и описать процедуру получения такой лицензии. Включите следующие шаги:

1. Определение требований: Исследуйте правовые и нормативно-технические требования, которые необходимо удовлетворить для получения лицензии. Объясните, какие документы и сертификаты необходимо предоставить.
2. Подготовка заявки: Разработайте образец заявки на получение лицензии. Укажите необходимую информацию, которую требуется предоставить, такую как контактные данные, квалификация персонала и прочее.
3. Сбор документов: Определите список необходимых документов и сертификатов, которые нужно предоставить вместе с заявкой. Объясните, какие документы нужно подготовить и где их можно получить.
4. Проверка соответствия: Опишите процесс проверки соответствия предоставленных документов требованиям для получения лицензии. Укажите, какие организации или органы будут осуществлять проверку.
5. Выдача лицензии: Объясните, как будет проводиться рассмотрение заявки и выдача лицензии. Укажите возможные сроки и условия получения лицензии.

Вопросы

1. Что такое лицензирование в контексте защиты информации?
2. Какие организации или учреждения выдают лицензии в области защиты информации?
3. Каковы основные требования для получения лицензии в области защиты информации?
4. Какие преимущества имеют организации, которые обладают лицензией на защиту информации?
5. Какие виды лицензий существуют в области защиты информации и как они различаются?
6. Какая роль играет государство в процессе лицензирования в области защиты информации?
7. Какие шаги необходимо предпринять для продления или обновления лицензии в области защиты информации?
8. Какие меры ответственности предусмотрены для организаций без лицензии в области защиты информации?
9. Как влияет лицензирование на доверие клиентов и партнеров к организации?
10. В чем разница между лицензированием в области защиты информации и сертификацией?
11. Существуют ли международные стандарты и требования для лицензирования в области защиты информации?
12. Какие особенности лицензирования существуют для разных отраслей или секторов?
13. Как можно проверить действительность и подлинность лицензии в области защиты информации?
14. Какие ограничения накладываются на организации без лицензии в области защиты информации?
15. Какова роль экспертов-аудиторов при процессе лицензирования в области защиты информации?

Самостоятельная работа №6 -
Сертификация в области защиты информации

Задание 2: Сертификация в области защиты информации

Тема: Процесс сертификации системы управления информационной безопасностью (СУИБ).

Описание задания:

Вы являетесь консультантом по информационной безопасности, и ваш клиент хочет сертифицировать свою систему управления информационной безопасностью (СУИБ) в соответствии с международным стандартом. Ваше задание состоит в том, чтобы провести и описать процесс сертификации СУИБ. Включите следующие шаги:

1. Изучение стандарта: Изучите выбранный международный стандарт по системам управления информационной безопасностью (например, ISO 27001). Объясните его основные принципы и требования.
2. Анализ текущего состояния: Оцените текущую систему управления информационной безопасностью вашего клиента и определите расхождения с требованиями стандарта. Составьте отчет о выявленных расхождениях и рекомендациях по их устранению.
3. Планирование сертификации: Разработайте план сертификации, включающий необходимые шаги, ресурсы, сроки и ответственных лиц. Объясните процесс подготовки к сертификации, включая разработку политик и процедур, проведение аудитов и обучение персонала.
4. Выполнение мероприятий: Укажите, какие действия должны быть выполнены для устранения расхождений с требованиями стандарта. Расскажите о процессе разработки и внедрения необходимых изменений в СУИБ.
5. Аудит и сертификация: Объясните процесс проведения аудита системы управления информационной безопасностью и выдачи сертификата соответствия стандарту. Укажите, кто будет проводить аудит и какие документы и информацию нужно предоставить во время аудита.

6. Сопровождение сертификата: Объясните процесс сопровождения сертификата и необходимые действия для его поддержания. Укажите периодичность повторных аудитов и обновления сертификата.

Вопросы:

1. Что такое сертификация в контексте защиты информации?
2. Какие организации проводят сертификацию в области защиты информации?
3. Каковы основные шаги или процедуры сертификации в области защиты информации?
4. Какие преимущества имеют организации, обладающие сертификатом в области защиты информации?
5. Какие виды сертификаций существуют в области защиты информации и как они различаются?
6. Какая роль играет государство в процессе сертификации в области защиты информации?
7. Какие требования нужно выполнить для получения сертификата в области защиты информации?
8. Какие меры ответственности предусмотрены для организаций без сертификата в области защиты информации?
9. Как сертификация влияет на доверие клиентов и партнеров к организации?
10. В чем разница между сертификацией и лицензированием в области защиты информации?
11. Существуют ли международные стандарты и требования для сертификации в области защиты информации?
12. Какая роль экспертов-аудиторов при процессе сертификации в области защиты информации?
13. Как можно проверить действительность и подлинность сертификата в области защиты информации?
14. Какие ограничения накладываются на организации без сертификата в области защиты информации?
15. Какие особенности сертификации существуют для разных отраслей или секторов?

Самостоятельная работа №7-8 -

Система правовой ответственности за утечку информации и утрату носителей информации. Правовые основы деятельности подразделений защиты информации

Нарушения, связанные с проведением служебных совещаний:

– проведение совещаний в не аттестованных помещениях без соответствующего разрешения руководителя предприятия или его заместителей;

– допуск на совещание лиц, не имеющих отношения к обсуждаемым вопросам и участие которых не вызывается служебной необходимостью;

– несоблюдение очередности рассмотрения вопросов конфиденциального характера;

– несоблюдение требований внутриобъектового режима при проведении совещаний;

– фотографирование, демонстрация конфиденциальных изделий, фильмов без согласования с СБ;

– звукозапись выступлений участников совещания на носителе, не учтенном в СБ;

– направление тетрадей (записей) секретного характера в учреждения, которых эти сведения непосредственно не касаются;

– недостаточное знание работниками, участвующими в приеме командированных лиц, требований инструкции о порядке приема командированных лиц (об этом заявили около 45% опрошенных лиц).

Задание по теме "Система правовой ответственности за утечку информации":

Исследуйте существующую систему правовой ответственности за утечку информации. Составьте доклад, в котором обоснуйте эффективность или неэффективность данной системы. Опишите основные проблемы и недостатки, а также предложите возможные пути улучшения системы правовой ответственности.

Задание по теме "Правовые основы деятельности подразделений защиты информации":

Проведите исследование о правовых основах деятельности подразделений защиты информации. Составьте отчет, в котором рассмотрите существующие нормативные акты и законодательство, регулирующие работу подразделений защиты информации. Опишите и проанализируйте основные обязанности и полномочия данных подразделений, а также выявите возможные проблемы и предложите меры для их решения и улучшения правовых основ деятельности подразделений защиты информации.

Вопросы:

Тема: Система правовой ответственности за утечку информации и утрату носителей информации

1. Каковы основные законы и нормативные акты, регулирующие систему правовой ответственности за утечку информации и утрату носителей информации в вашей стране?
2. Какие виды правовой ответственности применяются в случае утечки информации или утраты носителей информации?
3. Каковы критерии определения масштаба утечки информации или утраты носителей информации?
4. Какие меры предусмотрены для обеспечения конфиденциальности информации и предотвращения её утечки или утраты?
5. Каковы последствия правовой ответственности за утечку информации или утрату носителей информации для организаций или лиц, допустивших нарушение?
6. Какие санкции могут быть применены в случае утечки информации или утраты носителей информации?
7. Каковы механизмы выявления и расследования случаев утечки информации или утраты носителей информации?
8. Какая роль правоохранительных органов в системе правовой ответственности за утечку информации и утрату носителей информации?

9. Каковы особенности правовой ответственности за утечку информации или утрату носителей информации в сфере государственной безопасности?
10. Каковы международные стандарты и соглашения, регулирующие систему правовой ответственности за утечку информации или утрату носителей информации?
11. Какие меры могут быть предприняты для превентивной защиты от утечки информации или утраты носителей информации?
12. Каковы процедуры установления факта утечки информации или утраты носителей информации?
13. Каковы права и обязанности работников в контексте системы правовой ответственности за утечку информации или утрату носителей информации?
14. Какие меры предусмотрены для восстановления и компенсации ущерба, причиненного утечкой информации или утратой носителей информации?
15. Каковы перспективы развития системы правовой ответственности за утечку информации и утрату носителей информации?

Тема: Правовые основы деятельности подразделений защиты информации

1. Какие законы и нормативные акты регулируют деятельность подразделений защиты информации в вашей стране?
2. Каковы основные задачи и функции подразделений защиты информации?
3. Каковы права и полномочия сотрудников подразделений защиты информации?
4. Какие требования предъявляются к персоналу, работающему в подразделениях защиты информации?
5. Как организована система сертификации и аккредитации подразделений защиты информации?
6. Какие меры предусмотрены для обеспечения конфиденциальности информации в процессе её защиты?
7. Какие стандарты и методологии применяются в работе подразделений защиты информации?

8. Каковы особенности деятельности подразделений защиты информации в государственных организациях?

9. Каковы особенности деятельности подразделений защиты информации в коммерческих организациях?

10. Каковы требования к техническим средствам и программному обеспечению, используемым в работе подразделений защиты информации?

11. Каковы особенности правовой ответственности сотрудников подразделений защиты информации?

12. Какие меры принимаются для повышения квалификации и профессионального развития сотрудников подразделений защиты информации?

13. Каковы механизмы контроля и аудита деятельности подразделений защиты информации?

14. Каковы перспективы развития и совершенствования правовых основ деятельности подразделений защиты информации?

15. Каковы лучшие практики и опыт других стран в области правовых основ деятельности подразделений защиты информации?

Самостоятельная работа №9 -
Правовые основы защиты персональных данных.

Задание:

Напишите эссе на тему "Правовые основы защиты персональных данных". В вашем эссе рассмотрите следующие аспекты:

1. Законы и нормативные акты, регулирующие защиту персональных данных в вашей стране.
2. Определение понятия "персональные данные" и принципы их обработки.
3. Права субъектов персональных данных в контексте правовых основ защиты.
4. Обязанности организаций и лиц, обрабатывающих персональные данные.
5. Процедуры получения согласия на обработку персональных данных.
6. Механизмы обеспечения безопасности персональных данных.
7. Требования к передаче персональных данных третьим лицам.
8. Ответственность за нарушение правил обработки персональных данных.
9. Международные стандарты и соглашения по защите персональных данных.
10. Роль государственных органов в обеспечении защиты персональных данных.
11. Проблемы и вызовы в сфере правовой защиты персональных данных.
12. Действия при утечке персональных данных и меры предотвращения таких случаев.
13. Правовые основы защиты персональных данных в онлайн-среде и социальных сетях.
14. Роль образования и повышения осведомленности населения о правилах защиты персональных данных.

15. Перспективы развития законодательства по защите персональных данных.

Вопросы:

1. Какие законы и нормативные акты регулируют защиту персональных данных в вашей стране?
2. Что понимается под термином "персональные данные"?
3. Какие принципы обработки персональных данных должны соблюдаться?
4. Какие права имеют субъекты персональных данных?
5. Какие обязанности возлагаются на организации и лиц, обрабатывающих персональные данные?
6. Какие процедуры требуются для получения согласия на обработку персональных данных?
7. Каким образом обеспечивается безопасность персональных данных?
8. Каким требованиям должна соответствовать передача персональных данных третьим лицам?
9. Какая ответственность предусмотрена за нарушение правил обработки персональных данных?
10. Какие международные стандарты и соглашения действуют в области защиты персональных данных?
11. Какова роль государственных органов в обеспечении защиты персональных данных?
12. Какие проблемы и вызовы возникают в сфере правовой защиты персональных данных?
13. Каким образом следует действовать при утечке персональных данных и какие меры можно предпринять для их предотвращения?
14. Каковы основные правовые аспекты защиты персональных данных в онлайн-среде и социальных сетях?
15. Какое значение имеет образование и повышение осведомленности населения о правилах защиты персональных данных?
16. Какие перспективы развития законодательства по защите персональных данных вы видите в будущем?

Литература

1. Корнилова, А. А. Защита персональных данных : учебное пособие / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2020. – 119 с. – URL: https://biblioclub.ru/index.php?page=book&id=611314 (дата обращения: 04.05.2023). - Режим доступа: по подписке. – Текст : электронный.

2. Арзуманян, А. Б. Международные стандарты правовой защиты информации и информационных технологий : учебное пособие / А. Б. Арзуманян ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – 140 с. – URL: https://biblioclub.ru/index.php?page=book&id=612162 (дата обращения: 04.05.2023). – Режим доступа: по подписке. – Текст : электронный.

3. Информационная безопасность в цифровом обществе : учебное пособие / А. С. Исмагилова, И. В. Салов, И. А. Шагапов, А. А. Корнилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2019. – 128 с. – URL: https://biblioclub.ru/index.php?page=book&id=611084 (дата обращения: 04.05.2023). – Режим доступа: по подписке. – Текст : электронный.

4. Спеваков, А. Г. Основы правового обеспечения информационной безопасности : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013. - Ч. 1. - 150 с. - Текст : электронный.

5. Спеваков, А. Г. Основы правового обеспечения информационной безопасности : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013. - Ч. 2. - 303 с. - Текст : электронный.