Практическая работа №6 Асылбек уулу Бакыта из группы ИСП-308

1 Часть

1. Составьте перечень нормативно-правовых актов, регулирующих правоотношения в сфере информации.
   1. Конституция

Статья 23 определяет права на неприкосновенность частной жизни,

личную и семейную тайну, тайну переписки.

Статья 24 определяет права в области информации о частной жизни

лица.

Статья 29 определяет права в области свободы слова и информации.

Статья 44 определяет права в области культурной жизни и творчества.

* 1. Федеральные законы

Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ

Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ

Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ

Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ

Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ

* 1. Указы президента

Указ Президента РФ “Об утверждении доктрины информационной безопасности российской федерации” от 05.12.2016 N 646

Указ Президента РФ “Об утверждении перечня сведений конфиденциального характера” от 06.03.1997 N 188.

Указ Президента РФ “Об утверждении перечня сведений, отнесенных к государственной тайне” от 30.11.1995 N 1203.

Указ Президента РФ “Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела” от 30.05.2005 N 609.

Указ Президента РФ “О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации” от 15.01.2013 N 31с (Выписка).

Указ Президента РФ “Основные направления госполитики в области обеспечения безопасности АСУ П и ТП КВО инфраструктуры РФ” от 03.02.2012 N803.

Указ Президента РФ “О Стратегии развития информационного общества в РФ на 2017 — 2030 годы” от 09.05.2017 N 203.

Указ Президента РФ “О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена” от 17.03.2008 N 351.

Указ Президента РФ “Вопросы федеральной службы по техническому и экспортному контролю” от 16.08.2004 N 1085.

Указ Президента РФ “Вопросы Федеральной службы безопасности Российской Федерации” от 11.08.2003 N 960.

Указ Президента РФ “Об утверждении состава комиссии по экспортному контролю российской федерации” от 16.05.2017 N 211.

Указ Президента РФ “О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации” от 03.04.1995 N 334.

* 1. Постановления правительства РФ

Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»

Постановление Правительства Российской Федерации от 28 февраля 1996 г. № 226 «О государственном учете и регистрации баз и банков данных» (с изм. от 2 марта 2005 г.)

Постановление Правительства Российской Федерации от 22 октября 2007 г. № 689 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»

Постановление Правительства РФ от 6 ноября 2007 года № 758

«О государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий»

Постановление Правительства Российской Федерации от 25 декабря 2007 г. № 931 «О некоторых мерах по обеспечению информационного взаимодействия государственных органов и органов местного самоуправления при оказании государственных услуг гражданам и организациям»

Постановление Правительства Российской Федерации от 29 декабря 2007 г. № 947 «Об утверждении Правил разработки, апробации, доработки и реализации типовых программно-технических решений в сфере региональной информатизации»

Постановление Правительства Российской Федерации от 17 марта 2008 г. № 179 «Об утверждении Положения о пользовании сайтами в сети Интернет, на которых осуществляется проведение открытых аукционов в электронной форме, и требованиях к технологическим, программным, лингвистическим, правовым и организационным средствам обеспечения пользования указанными сайтами, а также к системам, обеспечивающим проведение открытых аукционов в электронной форме»

Постановление Правительства Российской Федерации от 28 марта 2008 г. № 215 «О Правительственной комиссии по федеральной связи и информационным технологиям»

Постановление Правительства Российской Федерации от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям»

Постановление Правительства Российской Федерации от 15 июня 2009 г. № 478 «О единой системе информационно-справочной поддержки граждан и организаций по вопросам взаимодействия с органами исполнительной власти и органами местного самоуправления с использованием информационно-телекоммуникационной сети Интернет»

Постановление Правительства РФ от 10 сентября 2009 г. N 723 «О порядке ввода в эксплуатацию отдельных государственных информационных систем»

* 1. Акты министерств и ведомств

Приказ Министерства информационных технологий и связи РФ от 9 января 2008 г. № 3

Приказ Министерства информационных технологий и связи РФ от 11 марта 2008 г. № 32

* 1. ГОСТы

ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»

Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения»

ГОСТ Р ИСО/МЭК 15408-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»

ГОСТ Р ИСО/МЭК 15408-2-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности»

ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности»

ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»

ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»

ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»

ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий»

ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер»

ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети»

ГОСТ Р ИСО/ТО 13569-2007 «Финансовые услуги. Рекомендации по информационной безопасности»

ГОСТ Р ИСО/МЭК 15026-2002 «Информационная технология. Уровни целостности систем и программных средств»

ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»

ГОСТ Р ИСО/МЭК 18045-2008 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»

ГОСТ Р ИСО/МЭК 19794-2-2005 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца - контрольные точки»

ГОСТ Р ИСО/МЭК 19794-4-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца»

ГОСТ Р ИСО/МЭК 19794-5-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица»

ГОСТ Р ИСО/МЭК 19794-6-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза»

ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»

ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство»

ГОСТ Р 51725.6-2002 «Каталогизация продукции для федеральных государственных нужд. Сети телекоммуникационные и базы данных. Требования информационной безопасности»

ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты»

ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения»

ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества»

ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»

ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»

2 Часть

Указ Президента РФ от 5 декабря 2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"

1. Национальными интересами РФ в информационной сфере являются:

* обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;
* обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время;
* развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;
* доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;
* содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве (п. 8 ч. 2).

1. Основные информационные угрозы, стоящие перед страной и

обществом:

* расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы;
* расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий;
* различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры;
* состояние информационной безопасности в области обороны страны характеризуется увеличением масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и ее союзников и представляющих угрозу международному миру, глобальной и региональной безопасности;
* состояние информационной безопасности в области государственной и общественной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств в отношении Российской Федерации, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации;
* состояние информационной безопасности в экономической сфере характеризуется недостаточным уровнем развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг. Остается высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран;
* состояние информационной безопасности в области науки, технологий и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий, низким уровнем внедрения отечественных разработок и недостаточным кадровым обеспечением в области информационной безопасности, а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности. При этом мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и отечественной продукции зачастую не имеют комплексной основы;
* состояние информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства характеризуется стремлением отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве. (п.10, 12, 13, 14, 15, 16, 17, 18, 19, ч. 3)

1. Стратегические цели обеспечения информационной безопасности в различных областях:

* стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;
* стратегическими целями обеспечения информационной безопасности в области государственной и общественной безопасности являются защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры;
* стратегическими целями обеспечения информационной безопасности в экономической сфере являются сведение к минимально возможному уровню влияния негативных факторов, обусловленных недостаточным уровнем развития отечественной отрасли информационных технологий и электронной промышленности, разработка и производство конкурентоспособных средств обеспечения информационной безопасности, а также повышение объемов и качества оказания услуг в области обеспечения информационной безопасности;
* стратегической целью обеспечения информационной безопасности в области науки, технологий и образования является поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности, отрасли информационных технологий и электронной промышленности;
* стратегической целью обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства является формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве. (п. 20, 22, 24, 26, 28, ч. 4)

1. Органы, входящие в систему обеспечения информационной безопасности: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности. (п. 33 ч.5)

Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегни развития информационного общества в Российской Федерации на 2017 - 2030 годы»

1. Общая характеристика Стратегии развития информационного общества в Российской Федерации.

Данная Стратегия определяет цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов. (п. 1 ч. 1)

1. Принципы Стратегии развития информационного общества в Российской Федерации:

* обеспечение прав граждан на доступ к информации;
* обеспечение свободы выбора средств получения знаний при работе с информацией;
* сохранение традиционных и привычных для граждан (отличных от цифровых) форм получения товаров и услуг;
* приоритет традиционных российских духовно-нравственных ценностей и соблюдение основанных на этих ценностях норм поведения при использовании информационных и коммуникационных технологий;
* обеспечение законности и разумной достаточности при сборе, накоплении и распространении информации о гражданах и организациях;
* обеспечение государственной защиты интересов российских граждан в информационной сфере. (п. 3 ч. 1)

1. Целью данной Стратегии является создание условий для формирования в Российской Федерации общества знаний. (п. 20 ч. 3)
2. Национальные интересы, обеспечивающиеся Стратегией развития информационного общества в Российской Федерации:

* развитие человеческого потенциала;
* обеспечение безопасности граждан и государства;
* повышение роли России в мировом гуманитарном и культурном пространстве;
* развитие свободного, устойчивого и безопасного взаимодействия граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления;
* повышение эффективности государственного управления, развитие экономики и социальной сферы;
* формирование цифровой экономики. (п. 21 ч. 3)

1. Направления развития российских информационных и коммуникационных технологий:

* конвергенция сетей связи и создание сетей связи нового поколения;
* обработка больших объемов данных;
* искусственный интеллект;
* доверенные технологии электронной идентификации и аутентификации, в том числе в кредитно-финансовой сфере;
* облачные и туманные вычисления;
* интернет вещей и индустриальный интернет;
* робототехника и биотехнологии;
* радиотехника и электронная компонентная база;
* информационная безопасность. (п. 36 ч. 3.3)

Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации"

1. Данный Федеральный закон регулирует отношения, возникающие при:

* осуществлении права на поиск, получение, передачу, производство и распространение информации;
* применении информационных технологий;
* обеспечении защиты информации. (ст. 1)

1. Виды информации в зависимости от порядка ее предоставления или распространения:

1. Открытая информация - информация, которая общедоступна, распространяется без ограничений и может быть получена любым желающим лицом.

2. Ограниченный доступ к информации - информация, доступ к которой ограничен в соответствии с законодательством, правилами или условиями использования, установленными владельцем информации.

3. Закрытая информация - информация, подлежащая специальной защите в соответствии с законодательством. К ней относятся государственные тайны, коммерческие тайны и персональные данные.

4. Персональные данные - любая информация, относящаяся к определенному физическому лицу (субъекту персональных данных), которая может быть использована для его идентификации.

5. Конфиденциальная информация - информация, доступ к которой ограничен в соответствии с законодательством или условиями соглашения о конфиденциальности. К ней относятся коммерческие тайны и персональные данные.

1. Алгоритм действий по ограничению доступа к информационным ресурсам, на которых неоднократно размешалась информация, распространяемая нарушением требований законодательства Российской Федерации.

Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"

1. Данным Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным. (глава 1, статья 1)
2. Принципы обработки персональных данных:

* обработка персональных данных должна осуществляться на законной и справедливой основе;
* обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
* не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
* обработке подлежат только персональные данные, которые отвечают целям их обработки;
* содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
* при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных, или неточных данных;
* хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. (глава 2, статья 5)

3 Часть

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № | ФИО | Группа | Оценка | | | | Итоговая оценка (средний бал с округлением до десятых) |
| Оформление презентации | Соответствие  требованиям к содержанию | Свободное владение материалом | Ответы на вопросы |
| 1 | Корнеев Валентин | ИСП-308 | 5 | 7 | 5 | 5 | 5 |
| 2 | Храменков Георгий | ИСП-308 | 5 | 7 | 5 | 5 | 5 |
| 3 | Угланов Мурад | ИСП-308 | 5 | 7 | 5 | 5 | 5 |
| 4 | Шарибжанов Рамис | ИСП-309 | 5 | 7 | 5 | 5 | 5 |
| 5 | Гребенников Леонид | ИСП-308 | 5 | 7 | 5 | 5 | 5 |
| 6 | Шахов Андрей | ИСП-309 | 5 | 7 | 5 | 5 | 5 |
| 7 | Каршибаев Жахонгир | ИСП-309 | 5 | 7 | 5 | 5 | 5 |
| 8 | Сафонов Максим | ИСП-308 | 5 | 7 | 5 | 5 | 5 |
| 9 | Гусев Станислав | ИСП-309 | 5 | 7 | 5 | 5 | 5 |
| 10 | Демёхин Даниил | ИСП-308 | 5 | 7 | 5 | 5 | 5 |
| 11 |  |  |  |  |  |  |  |