Организационное и правовое обеспечение информационной безопасности

Пушкин Павел Юрьевич, к.т.н.

is-irk@mail.ru

КБ-1 «Защита информации»

Структура учебной дисциплины:

8 – лекций;
8 – практических (семинарских) занятий;
40 часов на выполнение самостоятельной работы

Экзамен

6.1. Рекомендуемая литература

6.1.1. Основная литература

1. Тумбинская М. В., Петровский М. В.. Комплексное обеспечение информационной безопасности на предприятии [Электронный ресурс]:учебник. - Санкт-Петербург: Лань, 2019. - 344 с. – Режим доступа: https://e.lanbook.com/book/125739
2. Нестеров С. А.. Основы информационной безопасности [Электронный ресурс]:учебное пособие. - Санкт-Петербург: Лань, 2019. - 324 с. – Режим доступа: https://e.lanbook.com/book/114688

6.1.2. Дополнительная литература

1. Аверченков В. И., Рытов М. Ю.. Служба защиты информации: организация и управление [Электронный ресурс]:. - Москва: ФЛИНТА, 2011. - 186 с. – Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=44740
2. Новиков В. К.. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс]:. - Москва: Горячая линия-Телеком, 2017. - 176 с. – Режим доступа: https://e.lanbook.com/book/111084

6.2. Перечень программного обеспечения

1. Microsoft Windows. Договор №32009183466 от 02.07.2020 г.
2. Microsoft Office. Договор №32009183466 от 02.07.2020 г.

6.3. Перечень современных профессиональных баз данных и информационных справочных систем

1. Информационно-правовой портал ГАРАНТ http:// www.garant.ru
2. Консультант Плюс http:// www.consultant.ru
3. Сайт Федеральной службы по техническому и экспортному контролю России http://www.fstec.ru
4. Сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций http://www.rkn.gov.ru

1. Термины и определения в сфере ИБ

Входной контроль: проверяем свои знания

Информация -

Информационная система -

Автоматизированная система –

Информационно-вычислительная система (программно-технический комплекс) -

Автоматизированное рабочее место -

Несанкционированный доступ (несанкционированные действия) -

Входной контроль: проверяем свои знания

149-ФЗ -

152-ФЗ -

187-ФЗ -

98-ФЗ -

5485-1-ФЗ-

Входной контроль: проверяем свои знания

вид информации, защиту которой регламентируют документы (ПДн, КТ, ГТ, ГИР и т.п.):

Приказ ФСТЭК №21-

Приказ ФСТЭК №17-

Приказ ФСБ №378-

Приказ ФАПСИ №152-

СТР-К -

Входной контроль: проверяем свои знания

Приведите требования к СЗИ для защиты следующих категорий информации:

1. ПДн.
2. КТ.
3. Особой важности.
4. Государственные информационные ресурсы, обрабатываемые в ГИС

Входной контроль: проверяем свои знания

Информация - сведения (сообщения, данные) независимо от формы их представления;

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

Автоматизированная система - Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций. ГОСТ 34.003-90

Информационно-вычислительная система (программно-технический комплекс) - Совокупность данных (баз данных) и программ, функционирующих на вычислительных средствах как единое целое для решения определенных задач. ГОСТ Р 53622-2009

Автоматизированное рабочее место АРМ - Программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида. ГОСТ 34.003-90

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Разные определения в разных нормативных документах, отсутствие определений в ФЗ (проблема) :

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (№149-ФЗ)

КОНФИДЕНЦИАЛЬНОСТЬ (ИНФОРМАЦИИ [РЕСУРСОВ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ]): confidentiality состояние информации [ресурсов автоматизированной, информационной системы], при котором доступ к ней [к ним] осуществляют только субъекты, имеющие на него право. (РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ. Р 50.1.053-2005)

Конфиденциальная информация -информация, требующая защиты (Руководящий документ. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ)

Входной контроль: проверяем свои знания

149-ФЗ – от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»

152-ФЗ - от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

187-ФЗ - от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

98-ФЗ - от 29.07.2004 N 98-ФЗ «О коммерческой тайне»

5485-I-ФЗ- от 21 июля 1993 г. «О государственной тайне»

Входной контроль: проверяем свои знания

вид информации, защиту которой регламентируют документы (ПДн, КТ, ГТ, ГИР и т.п.):

Приказ ФСТЭК №21-от 18 февраля 2013 г. N 21 ОБ УТВЕРЖДЕНИИ СОСТАВА И СОДЕРЖАНИЯ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Приказ ФСТЭК №17- 11 февраля 2013 г. N 17ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Приказ ФСБ №378- от 10 июля 2014 г. N **378** "Об утверждении Состава и содержания организационных и технических мер по обеспечению **безопасности** персональных данных при их обработке в **информационных** системах»

Приказ ФСБ №366- от 24.07.2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам»

Приказ ФАПСИ №152-от 13 июня 2001 г. N **152** "Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам **связи** с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну".

СТР-К - «Специальные требования и рекомендации по технической защите конфиденциальной информации»

Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения». – М.: ГТК РФ, 1992. – 13 с.

Настоящий руководящий документ устанавливает термины и определения понятий в области защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.

Установленные термины **обязательны** для применения во всех видах документации.

Для каждого понятия установлен один термин.

Применение синонимов термина не допускается.

Основные термины и определения:

Доступ к информации - Ознакомление с информацией, ее обработка, в частности, копирование модификация или уничтожение информации

Правила разграничения доступа (ПРД) - Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

Несанкционированный доступ к информации (НСД) - Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Примечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем

Защита от несанкционированного доступа - предотвращение или существенное затруднение несанкционированного доступа

Субъект доступа - Лицо или процесс, действия которого регламентируются правилами разграничения доступа

Объект доступа - Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа

Уровень полномочий субъекта доступа – Совокупность прав доступа субъекта доступа

Матрица доступа - Таблица, отображающая правила разграничения доступа

информационная инфраструктура: Совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам.

информационная сфера: Совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

информационный процесс: Процесс создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.

информационная технология; ИТ: Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

объект информатизации: Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

автоматизированная система в защищенном исполнении; АС в защищенном исполнении: Автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или нормативных документов по защите информации.

аттестация автоматизированной системы в защищенном исполнении: Процесс комплексной проверки выполнения заданных функций автоматизированной системы по обработке защищаемой информации на соответствие требованиям стандартов и/или нормативных документов в области защиты информации и оформления документов о ее соответствии выполнению функции по обработке защищаемой информации на конкретном объекте информатизации.

Модель нарушителя правил разграничения доступа- Абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа

Комплекс средств защиты - Совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации

Система разграничения доступа - Совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах

Идентификатор доступа - Уникальный признак субъекта или объекта доступа

Пароль - Идентификатор субъекта доступа, который является его (субъекта) секретом

Идентификация - Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов

Аутентификация - Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности

Средство защиты от несанкционированного доступа - Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа

Модель защиты - Абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа

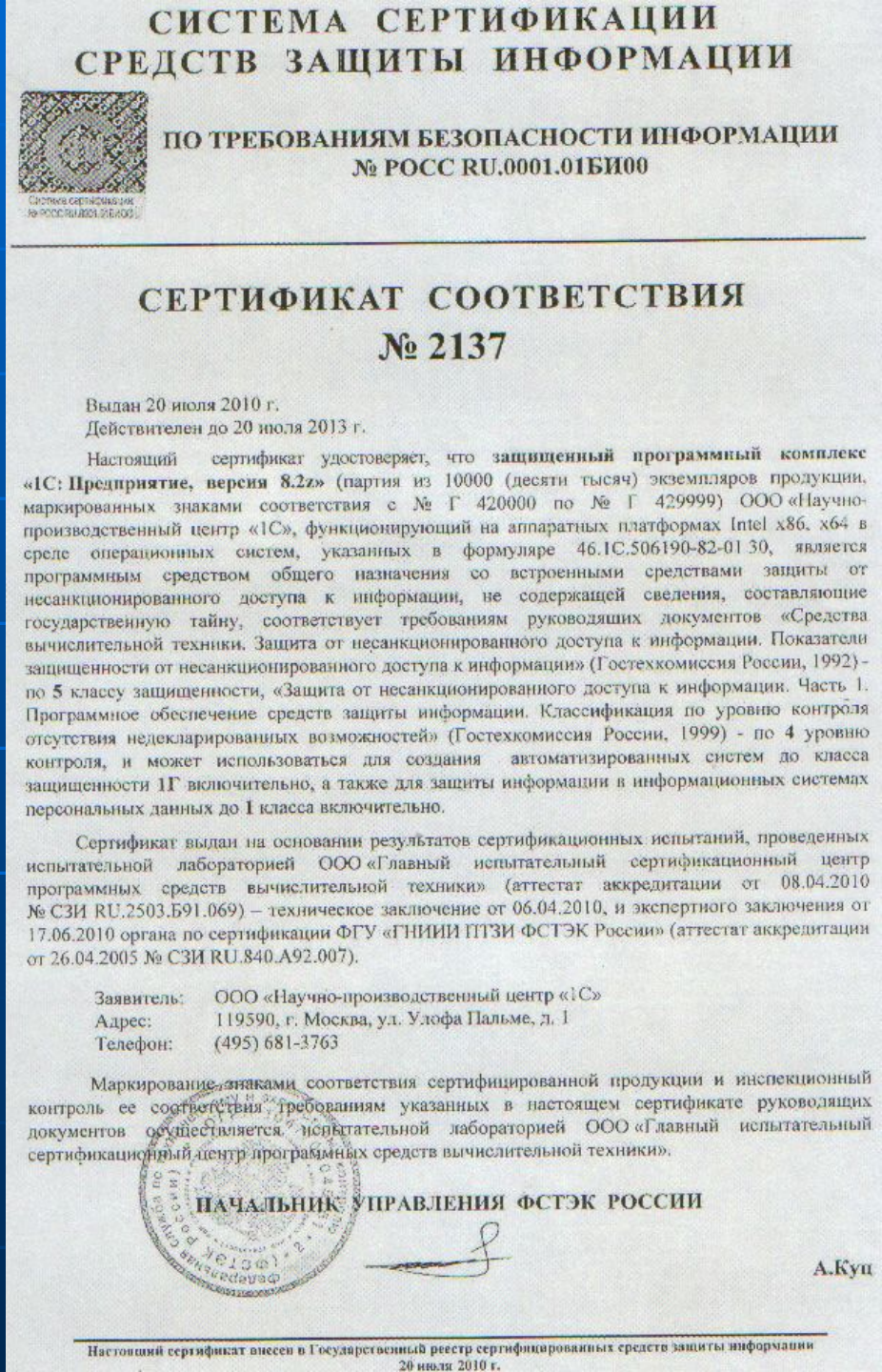
Целостность информации - Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения)

Класс защищенности средств вычислительной техники, автоматизированной системы - Определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации

Показатель защищенности средств вычислительной техники - Характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники

Система защиты информации от несанкционированного доступа - Комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах

Сертификат защиты - Документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 2137

Выдан 20 июля 2010 г.
Действителен до 20 июля 2013 г.

Настоящий сертификат удостоверяет, что **защищенный программный комплекс «1С: Предприятие, версия 8.2z»** (партия из 10000 (десяти тысяч) экземпляров продукции, маркированных знаками соответствия с № Г 420000 по № Г 429999) ООО «Научно-производственный центр «1С», функционирующий на аппаратных платформах Intel x86, x64 в среде операционных систем, указанных в формуляре 46.1С.506190-82-01 30, является программным средством общего назначения со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведения, составляющие государственную тайну, соответствует требованиям руководящих документов «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - по 5 классу защищенности, «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по 4 уровню контроля, и может использоваться для создания автоматизированных систем до класса защищенности 1Г включительно, а также для защиты информации в информационных системах персональных данных до 1 класса включительно.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «Главный испытательный сертификационный центр программных средств вычислительной техники» (аттестат аккредитации от 08.04.2010 № СЗИ RU.2503.Б91.069) – техническое заключение от 06.04.2010, и экспертного заключения от 17.06.2010 органа по сертификации ФГУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 26.04.2005 № СЗИ RU.840.А92.007).

Заявитель: ООО «Научно-производственный центр «1С»
Адрес: 119590, г. Москва, ул. Улофа Пальме, д. 1
Телефон: (495) 681-3763

Маркирование знаками соответствия сертифицированной продукции и инспекционный контроль ее соответствия требованиям указанных в настоящем сертификате руководящих документов осуществляется испытательной лабораторией ООО «Главный испытательный сертификационный центр программных средств вычислительной техники».

НАЧАЛЬНИК УПРАВЛЕНИЯ ФСТЭК РОССИИ А.Куц

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 20 июля 2010 г.

безопасность информации [данных]: Состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

защита информации; ЗИ: Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на (149-ФЗ):

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2) соблюдение конфиденциальности информации ограниченного доступа;
3) реализацию права на доступ к информации.

правовая защита информации: Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

организационные меры обеспечения информационной безопасности; организационные меры обеспечения ИБ: Меры обеспечения информационной безопасности, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации.

техническая защита информации; ТЗИ: Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

криптографическая защита информации: Защита информации с помощью ее криптографического преобразования.

физическая защита информации: Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

система защиты информации: Совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

политика безопасности (информации в организации): Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Политики должны содержать:

- предмет, основные цели и задачи политики безопасности;

- условия применения политики безопасности и возможные ограничения;

- описание позиции руководства организации в отношении выполнения политики безопасности и организации режима информационной безопасности организации в целом;

- права и обязанности, а также степень ответственности сотрудников за выполнение политики безопасности организации;

- порядок действия в чрезвычайных ситуациях в случае нарушения политики безопасности.

Определения из Федеральных законов

обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

доступ к информации - возможность получения информации и ее использования

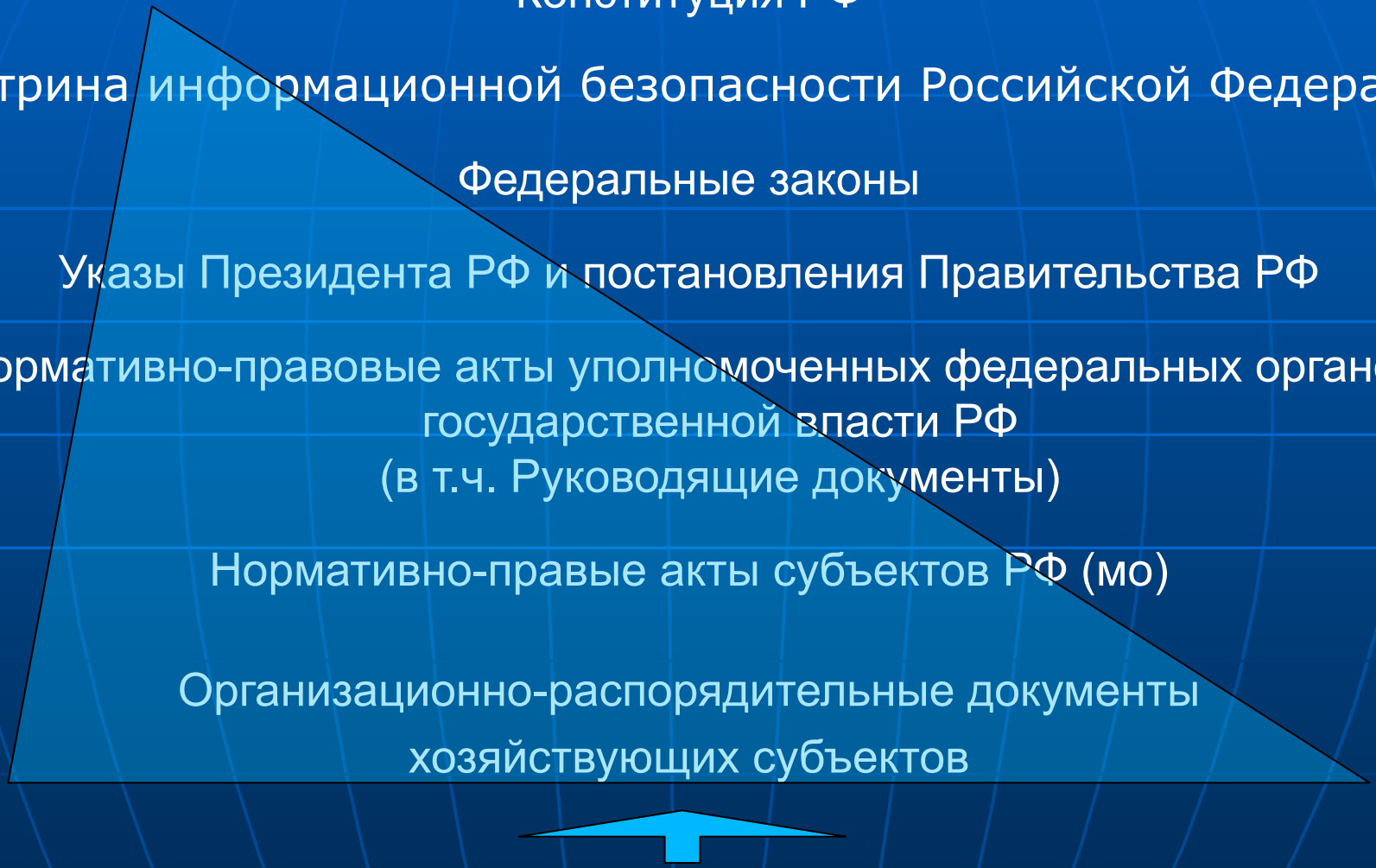
предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

Нормативная база по защите информации

Классификация нормативно-правовой базы по защите информации Российской Федерации:



Методические рекомендации ФОГВ,
ГОСТы и стандарты по защите информации

Основные НПА в области защиты информации

Федеральные законы

Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации»

Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных».

Федеральный закон от 06.04.2011 №63-ФЗ «Об электронной подписи».

Федеральный закон от 26.07.2017 N187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Федеральный закон от 21.07.1993 №5485-1 «О государственной тайне».

Федеральный закон от 29.07.2004 №98-ФЗ «О коммерческой тайне».

Иные Федеральные законы, ограничивающие доступ к информации

Указы Президента РФ

Указ Президента Российской Федерации № 188 от 6.03.1997 г. «Об утверждении перечня сведений конфиденциального характера»

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.
2. Сведения, составляющие тайну следствия и судопроизводства.
3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).
4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).
5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).
   Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.
6. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом от 2 октября 2007 г. N 229-ФЗ "Об исполнительном производстве".

Указ Президента РФ от 17 марта 2008 г. N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена"

Основное:

- при необходимости подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, к информационно-телекоммуникационным сетям международного информационного обмена такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данного требования является обязательным для операторов информационных систем, владельцев информационно-телекоммуникационных сетей и (или) средств вычислительной техники;

Указ Президента РФ от 22 мая 2015 г. N 260 "О некоторых вопросах информационной безопасности Российской Федерации"

Утверждает:
Порядок подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети "Интернет" и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети "Интернет"

gov.ru

RSNET

Постановления Правительства РФ

Принимаются в целях решения конкретных задач в области защиты информации:

-Лицензирование и сертификация;
-Защита различных категорий информации, информационных систем и объектов

Специальные нормативные документы:

- Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.
- Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.
- Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.
- Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 25 июля 1997 г.
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом председателя Гостехкомиссии России от 30 августа 2002 г. № 282.

- Руководящий документ. Приказ председателя Гостехкомиссии России от 19 июня 2002 г. N 187
  Безопасность информационных технологий. Критерии оценки безопасности информационных технологий;

- Руководящий документ. Приказ председателя Гостехкомиссии России от 4 июня 1999 г. N 114
  Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей

- Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г.
  Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации

Нормативные документы (стандарты)

Международные:

- ISO/IEC 27000:2009

Information technology - Security techniques - Information security management systems - Overview and vocabulary

Информационные технологии - Методы обеспечения безопасности - Системы менеджмента информационной безопасности - Определения и основные принципы;

- ISO/IEC 27001:2013

Information technology - Security techniques - Information security management systems - Requirements. Second edition 2013-10-01

Информационные технологии - Методы обеспечения безопасности - Системы менеджмента информационной безопасности - Требования. Вторая редакция 01.10.2013

- ISO/IEC 27002:2013
  Information technology - Security techniques - Code of practice for information security management. Second edition 2013-10-01
  Информационные технологии - Методы обеспечения безопасности - Практические правила управления информационной безопасностью. Вторая редакция 01.10.2013;

- ISO/IEC 27003:2010
  Information Technology - Security Techniques - Information Security Management Systems Implementation Guidance
  Информационные технологии - Методы обеспечения безопасности - Руководство по внедрению системы управления информационной безопасностью;

- ISO/IEC 27004:2009
  Information technology - Security techniques - Information security management - Measurement
  Информационные технологии - Методы обеспечения безопасности - Системы менеджмента информационной безопасности - Измерение

- ISO/IEC 27005:2011
  Information technology - Security techniques - Information security risk management. Second edition, 2011
  Информационные технологии - Методы обеспечения безопасности - Управление рисками информационной безопасности. Вторая редакция, 2011;

- ISO/IEC 27037:2012
  Information technology - Security techniques - Guidelines for identification, collection and/or acquisition and preservation of digital evidence
  Информационные технологии - Методы обеспечения безопасности - Руководство по идентификации, сбору и/или получению и обеспечению сохранности цифровых свидетельств;

- . . .

- ISO 27799:2008
  Health informatics - Information security management in health using ISO/IEC 27002
  Информатика в здравоохранении - Менеджмент безопасности информации по стандарту ISO/IEC 27002

Российские стандарты:

- ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России
- ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Госстандарт России
- ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России
- ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России
- ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения
- ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования
- ГОСТ Р 52069-2003. Защита информации. Система стандартов. Основные положения
- ГОСТ Р 53131-2008 (ИСО/МЭК ТО 24762-2008). Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения

- ГОСТ Р ИСО 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Госстандарт России
- ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Госстандарт России
- 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 13335-5-2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
- ГОСТ Р ИСО/МЭК 15408-1-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России
- ГОСТ Р ИСО/МЭК 15408-2-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России

- ГОСТ Р ИСО/МЭК 15408-3-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России
- ГОСТ Р ИСО/МЭК ТО 15443-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы
- ГОСТ Р ИСО/МЭК ТО 15443-2-2011. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 2. Методы доверия
- ГОСТ Р ИСО/МЭК ТО 15443-3-2011. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 3. Анализ методов доверия
- ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью
- ГОСТ Р ИСО/МЭК 18028-1-2008. Информационная технолоогия. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Менеджмент сетевой безопасности
- ГОСТ Р ИСО/МЭК ТО 19791-2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем

- ГОСТ Р ИСО/МЭК 27001-2006. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
- ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения
- ГОСТ Р ИСО/МЭК 27005-2009. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности
- ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции

Порядок использования НПБ

ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ

Основные положения

Информация как объект правовых отношений:

Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
2) использовать информацию, в том числе распространять ее, по своему усмотрению;
3) передавать информацию другим лицам по договору или на ином установленном законом основании;
4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;
2) принимать меры по защите информации;
3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Ограничение доступа к информации

1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.
2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.
3. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.
4. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.
5. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

6. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

7. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

9. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

Статья 16. Защита информации

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
2) своевременное обнаружение фактов несанкционированного доступа к информации;
3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
6) постоянный контроль за обеспечением уровня защищенности информации.

5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

Литература для самостоятельной работы:

Используемые в данной лекции НПА, российские и международные стандарты

Задание на самостоятельную работу для подготовки к семинарскому занятию:

1. Подготовить сообщение о видах тайн: название тайны/правовое основание (ФЗ с указанием ст., п., пп.)/сферы действия / основные требования к защите
2. Изучить термины и определения, рассмотренные на лекции
3. Составить перечень НПБ, необходимой для защиты ПДн, КТ, КИИ, ГИС:

ФЗ → УП → ПП → Приказы → Методические рекомендации