МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

Институт кибербезопасности и цифровых технологий

(наименование института, филиала)

Кафедра КБ-2«Прикладные информационные технологии»

(наименование кафедры)

ОТЧЕТ

по дисциплине: «Основы информационной безопасности»

Работа с правовыми актами, документами и стандартами ИБ

(задание)

Задание получил:

_1_ курс, группа _БИСО-02-23_ _23Б0667_

Шифр

_____Макаревич Сергей В._____

ФИО

Проверил:

«»____2023 г. _____

Дата *Подпись*

- _____

Отметка / результат *ФИО*

Москва 2023 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Была поставлена задачанаучиться работать в справочно-правовой системе с нормативными и правовыми документами по защите информации, а также провести обзор стандартов защиты информации и поработать с их содержанием. Цель также включает понимание стандартов по защите информации.

1 Теоретические вопросы

Теоретические вопросы:

1) Предмет и задачи программно-аппаратной защиты информации.

2) Основные понятия программно-аппаратной защиты информации.

3) Классификация методов и средств программно-аппаратной защиты информации.

4) Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

1.1 Перечень основных нормативных документов, регламентирующих деятельность области защиты информации

1.1.1 Конституция РФ

Статья 24:

Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются

Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 29:

Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом.

Статья 55:

Права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Статьи 22 и 23:

Конституции устанавливают конституционный запрет на произвольное вмешательство в частную жизнь каждого, а также запрет на осуществление сбора, хранения и использование информации о частной жизни лица, без его согласия.

1.1.2 Гражданский кодекс Российской Федерации

Статья 152. Защита чести, достоинства и деловой репутации:

1) Гражданин вправе требовать по суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший такие сведения не докажет, что они соответствуют действительности.

2) Сведения, порочащие честь, достоинство или деловую репутацию гражданина и распространенные в средствах массовой информации, должны быть опровергнуты в тех же средствах массовой информации.

3) В случаях, когда сведения, порочащие честь, достоинство или деловую репутацию гражданина, стали широко известны и в связи с этим опровержение невозможно довести до всеобщего сведения, гражданин вправе требовать удаления соответствующей информации, а также пресечения или запрещения дальнейшего распространения указанных сведений путем изъятия и уничтожения без какой бы то ни было компенсацииэкземпляров материальных носителей, содержащих указанные сведения.

4) Если сведения, порочащие честь, достоинство или деловую репутацию гражданина, оказались после их распространения доступными в сети "Интернет", гражданин вправе требовать удаления соответствующей информации,

Статья 152.1. Охрана изображения гражданина:

1) Обнародованиеи дальнейшее использование изображения гражданина допускаются только с согласия этого гражданина.

2) Если изображение гражданина, полученное или используемое с нарушением пункта 1 настоящей статьи, распространено в сети "Интернет", гражданин вправе требовать удаления этого изображения, а также пресечения или запрещения дальнейшего его распространения.

Статья 152.2. Охрана частной жизни гражданина:

1) Если иное прямо не предусмотрено законом, не допускаются без согласия гражданина сбор, хранение, распространение и использование любой информации о его частной жизни, в частности сведений о его происхождении, о месте его пребывания или жительства, о личной и семейной жизни.

2) Неправомерным распространением полученной с нарушением закона информации о частной жизни гражданина считается, в частности, ее использование при создании произведений науки, литературы и искусства, если такое использование нарушает интересы гражданина.

3) В случаях, когда информация о частной жизни гражданина, полученная с нарушением закона, содержится в документах, видеозаписях или на иных материальных носителях, гражданин вправе обратиться в суд с требованием об удалении соответствующей информации, а также о пресечении или запрещении дальнейшего ее распространения путем изъятия и уничтожения без какой бы то ни было компенсации изготовленных в целях введения в гражданский оборот экземпляров материальных носителей, содержащих соответствующую информацию.

Статья 727. Конфиденциальность полученной сторонами информации:

Если сторона благодаря исполнению своего обязательства по договору подряда получила от другой стороны информацию о новых решениях и технических знаниях, в том числе не защищаемых законом, а также сведения, в отношении которых их обладателем установлен режим коммерческой тайны, сторона, получившая такую информацию, не вправе сообщать ее третьим лицам без согласия другой стороны.(в ред. Федерального закона от 12.03.2014 N 35-ФЗ)

1.1.3 Уголовный Кодекс РФ

Глава 28. Преступления в сфере компьютерной информации

Статья 272. Неправомерный доступ к компьютерной информации

Неправомерный доступ к охраняемой законом компьютерной информации, копирование компьютерной информации наказывается.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, наказываются.

Статья 274.2. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования.

Нарушение порядка установки, эксплуатации и модернизации в сети связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети

связи общего пользования либо несоблюдение технических условий их установки или требований к сетям связи при использовании указанных технических средств наказывается.

Статья 138.1. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации

Незаконные производство, приобретение и (или) сбыт специальных технических средств, предназначенных для негласного получения информации, -наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Примечания:

1) Под специальными техническими средствами, предназначенными для негласного получения информации, в настоящем Кодексе понимаются приборы, системы, комплексы, устройства, специальные инструменты для проникновения в помещения и (или) на другие объекты и программное обеспечение для электронных вычислительных машин и других электронных устройств для доступа к информации и (или) получения информации с технических средств ее хранения, обработки и (или) передачи, которым намеренно приданы свойства для обеспечения функции скрытого получения информации либо доступа к ней без ведома ее обладателя.

2) К специальным техническим средствам, предназначенным для негласного получения информации, не относятся находящиеся в свободном обороте приборы, системы, комплексы, устройства, инструменты бытового назначения, обладающие функциями аудиозаписи, видеозаписи,

фотофиксации и (или) геолокации, с открыто расположенными на них органами управления таким функционалом или элементами индикации, отображающими режимы их использования, или наличием на них маркировочных обозначений, указывающих на их функциональное назначение, и программное обеспечение с элементами индикации, отображающими режимы его использования и указывающими на его функциональное назначение, если им преднамеренно путем специальной технической доработки, программирования или иным способом не приданы новые свойства, позволяющие с их помощью получать и (или) накапливать информацию, составляющую личную, семейную, коммерческую или иную охраняемую законом тайну, без ведома ее обладателя. (примечания введены Федеральным законом от 02.08.2019 N 308-ФЗ)

Статья 159.6. Мошенничество в сфере компьютерной информации

Нарушение порядка установки, эксплуатации и модернизации в сети связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования либо несоблюдение технических условий их установки или требований к сетям связи при использовании указанных технических средств наказывается.

УК РФ Статья 159.6. Мошенничество в сфере компьютерной информации(введена Федеральным законом от 29.11.2012 N 207-ФЗ).

1) Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, -наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными

работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев.

2) То же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, - наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до пяти лет с ограничением свободы на срок до одного года или без такового.(в ред. Федерального закона от 03.07.2016 N 325-ФЗ)

3) Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные:

- лицом с использованием своего служебного положения;

- в крупном размере;

- с банковского счета, а равно в отношении электронных денежных средств, -наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.(часть 3 в ред. Федерального закона от 23.04.2018 N 111-ФЗ)

4) Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо

крупном размере, -наказываются лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

1.1.4 Доктрина информационной безопасности РФ

Даёт определение следующим понятиям: национальные интересы Российской Федерации, угрозы информационной безопасности Российской Федерации, информационная безопасность Российской Федерации, информационная инфраструктура Российской Федерации. (Глава I, п. 2)

Определяет основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации. (Глава I, п. 3)

Определяет информационные технологии фактором ускорения экономического развития государства и формирования информационного общества. (Глава II, п. 7)

Определяет следующие национальные интересы в информационной сфере:

1) Обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации;

2) Обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры;

3) Развитие в Российской Федерации отрасли информационных технологий и электронной промышленности;

4) Содействие формированию системы международной информационной безопасности. (Глава I, п. 8)

Главой III определяет основные информационные угрозы:

1) Наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях;

2) Расширение масштабов использования специальными службамиотдельных 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.

3) Наращивание информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.

4) Увеличение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий.

Главой IV определяются цели и основные направления обеспечения информационной безопасности:

В соответствии с военной политикой Российской Федерации основными направлениями обеспечения информационной безопасности в области обороны страны являются:

а) стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий;

б) совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства;

в) прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере;

г) содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере;

д) нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества.

Защита жизненно важных интересов личности, прогнозирование информационных угроз, сдерживание и предотвращение военных конфликтов, защита суверенитета и поддержание политической и социальной стабильности, территориальной целостности Российской Федерации.

1.1.5 Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1

Ст. 5 определяет перечень сведений, составляющих государственную тайну:

1) Сведения в военной области: о содержании стратегических планов, о планах строительства ВС РФ, о разработке, производстве и утилизации ядерных боеприпасов, о дислокации, назначении и степени готовности особо важных объектов и др.

2) Сведения в области экономики, науки и техники: о силах и средствах гражданской обороны, об объемах государственного оборонного заказа, о достижениях науки и техники, о запасах металлов платиновой группы и др.

3) Сведения в области внешней политики и экономики: о внешнеполитической и внешнеэкономической деятельности Российской Федерации, о финансовой политике в отношении иностранных государств, о расходах федерального бюджета и др.

Ст. 20 определяет органы защиты государственной тайны:

Межведомственная комиссия по защите государственной тайны, органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны и др.

Ст. 26 устанавливается ответственность за нарушение законодательства РФ о государственной тайне:

Уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.

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

Ст.3 определяются принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации**.**

Оно основывается на свободе поиска, производства и распространения информации, установлении ограничений доступа к информации только федеральными законами, открытости информации о деятельности государственных органов и др.

Ст.5 определяется перечень сведений, составляющих гостайну. Гостайну составляют:

1) Сведения в военной области;
2) Сведения в области экономики, науки и техники;
3) Сведения в области внешней политики и экономики;
4) Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму.

Ст.12 описываются области государственного регулирования в сфере применения информационных технологий:

Регулирование отношений, связанных с поиском, производством и получением информации с применением информационных технологий,

развитие информационных систем различного назначения для обеспечения граждан.

Ст.16 описывает способы защиты информации.

Среди них принятие правовых, организационных и технических мер, направленных на: обеспечение защиты информации от неправомерного доступа, копирования, распространения и др. неправомерных действий в отношении информации, соблюдение конфиденциальности информации ограниченного доступа, реализация права на доступ к информации.

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

Ст.3 определяются основные понятия, используемые в федеральном законе: персональные данные, оператор, обработка персональных данных, обезличивание персональных данных и др.

Ст.6 устанавливаются условия обработки персональных данных:

Осуществляется с согласия субъекта персональных данных на обработку его персональных данных, необходима для защиты жизни, здоровья и иных жизненно важных интересов субъекта.

Ст.24 предусматривается ответственность за нарушение требований настоящего Федерального закона. Моральный вред, причинённый субъекту, подлежит возмещению в соответствии с законодательством Российской Федерации.

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

Ст.2 определяются основные понятия, используемые в федеральном законе:

Электронная подписьинформация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию), сертификат ключа проверки электронной подписи(электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи), ключ электронной подписи, удостоверяющий центр и др.

Ст.3 устанавливается правовое регулирование отношений в области использования электронных подписей.

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

Ст.3 определяются основные понятия, используемые в федеральном законе:

Коммерческая тайнарежим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду), контрагент(сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию) и др.

Ст.10 устанавливает меры по охране конфиденциальности информации, принимаемые ее обладателем:

Определение перечня информации, составляющей коммерческую тайну, учет лиц, получивших доступ к информации, ограничение доступа к информации, составляющей коммерческую тайну.

Ст.14 предусматривается ответственность за нарушение требований настоящего Федерального закона:

Дисциплинарную,гражданско-правовую,административнуюилиуголовнуюответственность в соответствии с законодательством Российской Федерации.

1.1.10 Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне»

Определяет перечень сведений, отнесенных к государственной тайне: сведения в военной области, сведения в области экономики, науки и техники, сведения в области внешней политики и экономики, сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, в области противодействия терроризму и обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты.

1.1.11 Указ Президента РФ от 6 марта 1997 г. №188 «Об утверждении перечня сведений конфиденциального характера»

Определяет перечень сведений, относящихся к сведениям конфиденциального характера: Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, служебные сведения, сведения о коммерческой деятельности, личные дела осужденных и т.д.

1.1.12 Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных (далее - информационные системы) и уровни защищенности таких данных.

Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных.

Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

1.1.13 Постановление Правительства РФ от 03.02.2012 N 79 (ред. от 26.11.2021) "О лицензировании деятельности по технической защите конфиденциальной информации" (вместе с "Положением о лицензировании деятельности по технической защите конфиденциальной информации")

Определяет порядок лицензирования деятельности по технической защите конфиденциальной информации, осуществляемой юридическими лицами и индивидуальными предпринимателями.

При осуществлении лицензируемого вида деятельности лицензированию подлежат: услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам, услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации, услуги по мониторингу информационной безопасности средств и систем информатизации, работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите

информации, услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации.

1.1.14 Приказ от 11 февраля 2013г. № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"

В документе устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информации в целях ее добывания, уничтожения, искажения или блокирования доступа к ней при обработке указанной информации в государственных информационных системах.

Определяет требования к организации защиты информации, содержащейся в информационной системе: разработка системы защиты, аттестация информационной системы и ввод ее в действие, обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы, ограничения программной среды, защита машинных носителей информации, обнаружение вторжение, защита среды виртуализации, защита технических средств.

1.1.15 Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Определяет состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с

учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий. В него входят:

1) Идентификация и аутентификация субъектов доступа и объектов доступа;

2) Управление доступом субъектов доступа к объектам доступа, ограничение программной среды;

3) Защита машинных носителей информации, на которых хранятся и обрабатываются персональные данные, регистрация событий безопасности, антивирусная защита, обнаружение (предотвращение) вторжений, контроль (анализ) защищенности персональных данных, обеспечение целостности информационной системы и персональных данных, обеспечение доступности персональных данных, защита среды виртуализации и др.

Руководящие документы ФСТЭК по защите от НСД:

Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

Устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов.

Необходимыми исходными данными для проведения классификации конкретной АС являются:

1) Перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;

2) Перечень лиц, имеющих доступ к штатнымсредствам АС, с указанием их уровня полномочий;

3) Матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;

4) Режим обработки данных в АС.

Руководящие документы ФСТЭК по защите от НДВ:

Руководящий документ. Приказ председателя Гостехкомиссии России от 4 июня 1999 г. N 114

Устанавливает классификацию программного обеспечения (ПО), защиты информации (СЗИ), в том числе и встроенных в общесистемное и прикладное ПО.

Документ предназначен для специалистов испытательных лабораторий, заказчиков, разработчиков ПО СЗИ при его контроле в части отсутствия недекларированных возможностей.

Положение по аттестации объектов информатизации по требованиям безопасности информации от 25 ноября 1994 г.

Устанавливает основные принципы, организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.

Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)

Устанавливает порядок организации работ, требования и рекомендации по обеспечению технической защиты конфиденциальной информации на территории Российской Федерации и является основным руководящим документом в этой области для федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, предприятий, учреждений и организаций, должностных лиц и граждан Российской Федерации, взявшим на себя обязательства либо обязанными по статусу исполнять требования правовых документов Российской Федерации по защите информации.

2 Задание №1

Нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными ипрограммно-аппаратными средствами:

2.1 Федеральный закон РФ от 27.06.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»

Статья 16. Защита информации:

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;

7) Нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

2.2 Федеральный закон РФ от 07.07.2003 № 126-ФЗ «О связи»

Статья 41. Подтверждение соответствия средств связи и услуг связи:

Для обеспечения целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации является обязательным подтверждение соответствия установленным требованиям средств связи, используемых в:

1) сети связи общего пользования;

2) технологических сетях связи и сетях связи специального назначения в случае их присоединения к сети связи общего пользования.

Операторы связи обязаны обеспечивать реализацию установленных федеральным органом исполнительной власти в области связи по согласованию с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, требований к сетям и средствам связи для проведения этими органами в случаях, установленных федеральными законами, мероприятий в целях реализации возложенных на них задач, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения указанных мероприятий.

2.3 Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных»

Статья 18. Обязанности оператора при сборе персональных данных:

При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на

территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона.

Обеспечение безопасности персональных данных достигается, в частности:

1) Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) Учетом машинных носителей персональных данных;

6) Обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

(в ред. Федерального закона от 30.12.2020 N 515-ФЗ)

7) Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Статья 6. Условия обработки персональных данных:

В поручении оператора должны быть определены перечень персональных данных, перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных, требования, предусмотренные частью 5 статьи 18 настоящего Федерального закона, обязанность по запросу оператора персональных данных в течение срока действия поручения оператора, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, установленных в соответствии с настоящей статьей, обязанность обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 настоящего Федерального закона.

2.4 Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Требования к защите персональных данных при их обработке в информационных системах персональных данных:

Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

1) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

2) обеспечение сохранности носителей персональных данных;

3) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

4) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 13 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 14 настоящего документа, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

Для обеспечения 1-го уровня защищенности персональных данных при ихобработке в информационных системах помимо требований, предусмотренных пунктом 15 настоящего документа, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

2.5 Руководящий документ. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»(утв. Решением Гостехкомиссии России от 30.03.1992)

Требования к классу защищенности 3Б (задания по безопасности):

Подсистема управления доступом:

Должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов.

Подсистема регистрации и учета:

Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.

В параметрах регистрации указываются:

а) дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

б) должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку).

Подсистема обеспечения целостности:

Должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды.

При этом:

а) целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;

б) целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

в) должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

г) должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;

д) должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

3 Задание №2

Федеральный закон РФ от 27.06.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»

Требования и рекомендации по защите информации программными и программно-аппаратными средствами:

Статья 16. Защита информации:

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

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

б) соблюдение конфиденциальности информации ограниченного доступа;

в) 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:

а) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

б) своевременное обнаружение фактов несанкционированного доступа к информации;

в) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

г) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

д) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

е) постоянный контроль за обеспечением уровня защищенности информации;

ж) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

(п. 7 введен Федеральным законом от 21.07.2014 N 242-ФЗ)

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.

4 Задание №3

Приказ ФСТЭК России от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Требования и рекомендации по защите информации программными и программно-аппаратными средствами.

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

1) Идентификация и аутентификация субъектов доступа и объектов доступа;

2) Управление доступом субъектов доступа к объектам доступа;

3) Ограничение программной среды;

4) Защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

5) Регистрация событий безопасности;

6) Антивирусная защита;

7) Обнаружение (предотвращение) вторжений;

8) Контроль (анализ) защищенности персональных данных;

9) Обеспечение целостности информационной системы и персональных данных;

10) Обеспечение доступности персональных данных;

11) Защита среды виртуализации;

12) Защита технических средств;

13) Защита информационной системы, ее средств, систем связи и передачи данных;

14) Выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

15) Управление конфигурацией информационной системы и системы защиты персональных данных(п.8)

Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:

1) Определение базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных в соответствии с базовыми наборами мер по обеспечению безопасности персональных данных, приведенными в приложении к настоящему документу;

2) Адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

3) Уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных с учетом не выбранных ранее мер, приведенных в приложении к настоящему документу, в результате чего определяются меры по обеспечению безопасности персональных данных, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных для конкретной информационной системы;

4) Дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации (п.9)

5) Могут применяться следующие меры:

a) Проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;

b) Тестирование информационной системы на проникновения;

c) Использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования (п.11)

5 Задание №4

Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные руководством Центра ФСБ России 21.02.2008 №149/6/6-622.

Выписать требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Безопасность обработки персональных данных с использованием криптосредств организуют и обеспечивают операторы, а также лица, которым на основании договора оператор поручает обработку персональных данных, и (или) лица, которым на основании договора оператор поручает оказание услуг по организации и обеспечению безопасности обработки в информационной системе персональных данных с использованием криптосредств.

При разработке и реализации мероприятий по организации и обеспечению безопасности персональных данных при их обработке в информационной системе оператор или уполномоченное оператором лицо осуществляет:

1) Разработку для каждой информационной системы персональных данных модели угроз безопасности персональных данных при их обработке;

2) Разработку на основе модели угроз системы безопасности персональных данных, обеспечивающей нейтрализацию всех перечисленных в модели угроз;

3) Определение необходимости использования криптосредств для обеспечения безопасности персональных данных и, в случае положительного решения, определение на основе модели угроз цели использования

криптосредств для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных и (или) иных неправомерных действий при их обработке;

4) Установку и ввод в эксплуатацию криптосредств в соответствии с эксплуатационной и технической документацией к этим средствам;

5) Проверку готовности криптосредств к использованию с составлением заключений о возможности их эксплуатации;

6) Обучение лиц, использующих криптосредства, работе с ними;

7) Поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных;

8) Учет лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационной системе (пользователи криптосредств);

9) Контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;

Пользователи криптосредств обязаны:

1) Не разглашать информацию, к которой они допущены, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты;

2) Соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним;

3) Сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;

4) Немедленно уведомлять оператора о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений,

хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных;

5) Сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящими Требованиями, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств.

Пользователи криптосредств обязаны:

1) Не разглашать информацию о ключевых документах;

2) Не допускать снятие копий с ключевых документов;

3) Не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;

4) Не допускать записи на ключевой носитель посторонней информации;

5) Не допускать установки ключевых документов в другие ПЭВМ (п.3)

Требования ФСТЭК по защите информации:

Выполнение требований регулятора по технической защите информации обязательно при:

1) Оказании услуг информационной безопасности (ТЗКИ, СКЗИ);

2) Проведении работ по обеспечению государственной и банковской тайн;

3) Выполнении обязанностей оператора персональных данных (ПНд);

4) Передаче информации посредством сети Интернет.

Требования ФСТЭК по технической защите информации распространяются на:

1) Программное обеспечения и оборудование;

2) Внешние носители;

3) Средства связи и шифровки/дешифровки данных;

4) Операционные системы;

5) Прочие технические средства хранения, обработки, передачи сведений;

6) Персональные данные;

7) Специалистов по обеспечению информационной безопасности.

Меры по защите персональных данных согласно требованиям ФСТЭК входят:

1) Использование системы идентификации и аутентификации (авторизации) субъектов, имеющих доступ к ПНд, и объектов ПНд;

2) Возможность ограничения и управления правами доступа к персональной информации;

3) Физическая и программная защита носителей информации;

4) Регистрация событий безопасности и ведение их журнала;

5) Применение средств антивирусной защиты;

6) Регулярный контроль защищенности ПНд;

7) Обнаружение и предотвращение вторжений, несанкционированного доступа;

8) Обеспечение доступности хранимых сведений, их и информационной системы, базы данных доступности;

9) Соблюдение требований по защите среды виртуализации, технических средств, информационной системы (ИС), ее средств, каналов и линий связи и передачи данных.

Требования ФСТЭК к специалистам по защите информации включают в себя понимание:

1) Основных законодательных и нормативных актов в области информационной безопасности и защиты персональных данных;

2) В области сертификации средств защиты информации;

3) О государственной системе противодействия иностранным техническим разведкам.

4) К профессиональным знаниям специалистов относится:

5) Подготовка в части работы с каналами и линиями связи (предотвращение утечки информации);

6) Ориентация в сфере комплексных СЗИ;

7) Понимание основ методологии построения СЗИ;

8) Умение работать со средствами контроля защищенности баз данных (БД) и т.д.

ЗАКЛЮЧЕНИЕ

В ходе выполнения поставленной задачи по изучению справочно-правовой системы, анализу нормативных документов и обзору стандартов защиты информации, были успешно приобретены необходимые навыки и знания. Полученные компетенции в области информационной безопасности позволят эффективно применять соответствующие методы и стандарты, повышая уровень защиты информационных ресурсов.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

Нормативные документы:

1. Конституция Российской Федерации;
2. Уголовный Кодекс Российской Федерации;
3. Доктрина информационной безопасности Российской Федерации;
4. Федеральный закон РФ от 21.07.1993 № 5485-1 «О государственной тайне»;
5. Федеральный закон РФ от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
6. Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных»;
7. Федеральный закон РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
8. Федеральный закон от 29.04.2004 № 98-ФЗ «О коммерческой тайне»;
9. Указы Президента Российской Федерации:
   - 9.1 Указ Президента РФ от 30 ноября 1995 г. №1203 «Об утверждении перечня сведений, отнесенных к государственной тайне»;
   - 9.2 Указ Президента РФ от 6 марта 1997 г. №188 «Об утверждении перечня сведений конфиденциального характера»;
10. Постановления Правительства Российской Федерации:
    - 10.1 Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

10.2 Постановление Правительства РФ от 03.02.2012 № 79 "О лицензировании деятельности по технической защите конфиденциальной информации";

11 Приказ от 11 февраля 2013г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

12 Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасностиперсональных данных при их обработке в информационных системах персональных данных»;

13 Руководящие документы ФСТЭК по защите от НСД;

14 Руководящие документы ФСТЭК по защите от НДВ;

15 Положение по аттестации объектов информатизации по требованиям безопасности информации от 25 ноября 1994 г.;

16 Специальные требования и рекомендации потехнической защите конфиденциальной информации (СТР-К);

17 Приказ ФСБ РФ от 9 февраля 2005г. № 66 «Об утверждении, разработке, производстве, реализации и эксплуатации шифровальных и криптографических средств защиты (Положение ПКЗ-2005»).

18 Положение по аттестации объектов информатизации по требованиям безопасности информации от 25 ноября 1994 г.;

19 Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К);

20 Приказ ФСБ РФ от 9 февраля 2005г. № 66 «Об утверждении, разработке, производстве, реализации и эксплуатации шифровальных и криптографических средств защиты (Положение ПКЗ-2005»);

21 Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для

обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. ФСБ РФ 21.02.2008 N 149/6/6-622).