

Организационное и правовое обеспечение информационной безопасности

Практическое занятие

ОПРЕДЕЛЕНИЕ ПЕРЕЧНЯ ОРГАНИЗАЦИОННЫХ МЕР ПО ЗАЩИТЕ ИСПДН

Методические рекомендации

по подготовке и проведению практического занятия

Цель занятия: получить навыки определения организационных мер по защите информации на основе нормативно-правовых документов

Теоретические сведения

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.

Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

Организационные меры устанавливаются организационно-распорядительными документами – вид письменного документа, в котором фиксируют решение административных и организационных вопросов, а также вопросов управления, взаимодействия, обеспечения и регулирования деятельности органов власти, учреждений, предприятий, организаций, их подразделений и должностных лиц (ГОСТ Р 6.30-2003).

К организационно-правовым мерам относят правовую защиту 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.

Технические меры по защите информации включают в себя ТЗИ, криптографическую и физическую защиту объектов 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.

Отчет о выполнении практической работы должен содержать:

- наименование практического занятия;
- цели занятия;
- перечень нормативных актов с терминами в области информационной безопасности;
- полные определения выбранных для построения системы понятий терминов;
- построенная система понятий для выбранных терминов в виде перечня и диаграмм;
- выводы о проделанной работе;
- список используемых в работе средств, в том числе информационных систем и ресурсов, литературы.

Порядок выполнения практической работы

1. На самостоятельной работе изучить термины и определения, касающиеся общих мер по защите информации, постановление Правительства РФ №1119, Приказ ФСТЭК России №21 [1, 2, 3, 4].

2. Изучить краткие теоретические сведения, указанные в настоящих рекомендациях.

3. Открыть официальный сайт ФСТЭК России <https://fstec.ru/> [5]. Найти в разделе «Документы» Приказ ФСТЭК №21.

4. Изучить содержание мер по защите ИСПДн, указанные в приложении к Приказу ФСТЭК №21. Выделить мероприятия, которые можно реализовать организационными мерами по защите информации. Результаты занести в таблицу в столбцы 1, 2, 3, 4 (в отчете используйте альбомную ориентацию).

5. Таблица 1

| № п/п | № меры/(УЗ ИСПДн) | Содержание меры | Способ реализации | Индекс УБИ | Наименование УБИ | Тип нарушения | Нарушение Конф/Цел/Дост | Примечание |
|-------|--------------------|---|--|------------|--|--|-------------------------|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1 | ОПС.3 (1, 2, 3, 4) | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компоненто в | Утверждение перечня типового ПО в организации, ограничение, разработка СРД (утверждение матрицы доступа) | УБИ. 023 | Угроза изменения компонентов информационной (автоматизированной) системы | Внутренний нарушитель с низким потенциалом | К/Ц/Д | Возможен контроль с использованием СЗИ, антивирусных средств, системного и прикладного ПО |
| | | | | | | | | |

6. В столбце 4 Таблицы 1 предложить способы реализации рассматриваемой меры.

7. Столбцы 5, 6, 7, 8, 9 Таблицы 1 заполняются с учетом сведений, указанных в БДУ ФСТЭК России <https://bdu.fstec.ru/>.

8. Сделайте выводы о проделанной работе.

Список источников:

1. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения <http://docs.cntd.ru/document/1200058320>.

2. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения <http://docs.cntd.ru/document/1200075565>.

3. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
http://www.consultant.ru/document/cons_doc_LAW_137356/

4. Приказ ФСТЭК России от 18 февраля 2013 г. №21
<https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy>

5. Сайт ФСТЭК России. <https://fstec.ru/>.

Приложение

СОСТАВ И СОДЕРЖАНИЕ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, НЕОБХОДИМЫХ ДЛЯ ОБЕСПЕЧЕНИЯ КАЖДОГО ИЗ УРОВНЕЙ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

| Условное обозначение и номер меры | Содержание мер по обеспечению безопасности персональных данных | Уровни защищенности персональных данных | | | |
|--|--|---|---|---|---|
| | | 4 | 3 | 2 | 1 |
| I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | | | | | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | + | + | + | + |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных | | | + | + |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | + | + | + | + |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | + | + | + | + |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | + | + | + | + |
| ИАФ.6 | Идентификация и аутентификация пользователей, | + | + | + | + |

| | | | | | |
|--|---|---|---|---|---|
| | не являющихся работниками оператора (внешних пользователей) | | | | |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) | | | | | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | + | + | + | + |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | + | + | + | + |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами | + | + | + | + |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | + | + | + | + |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | + | + | + | + |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | + | + | + | + |
| УПД.7 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных | | | | |
| УПД.8 | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему | | | | |
| УПД.9 | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы | | | | |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени | | + | + | + |

| | | | | | |
|--|---|---|---|---|---|
| | бездействия (неактивности) пользователя или по его запросу | | | | |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации | | + | + | + |
| УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки | | | | |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | + | + | + | + |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | + | + | + | + |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | + | + | + | + |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | + | + | + | + |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники | | | + | + |
| III. Ограничение программной среды (ОПС) | | | | | |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения | | | | |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения | | | + | + |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов | | | | + |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, | | | | |

| | | | | | |
|---|--|---|---|---|---|
| | удаление временных файлов | | | | |
| IV. Защита машинных носителей персональных данных (ЗНИ) | | | | | |
| ЗНИ.1 | Учет машинных носителей персональных данных | | | + | + |
| ЗНИ.2 | Управление доступом к машинным носителям персональных данных | | | + | + |
| ЗНИ.3 | Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны | | | | |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах | | | | |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных | | | | |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители персональных данных | | | | |
| ЗНИ.7 | Контроль подключения машинных носителей персональных данных | | | | |
| ЗНИ.8 | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания | | + | + | + |
| V. Регистрация событий безопасности (РСБ) | | | | | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | + | + | + | + |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + | + | + | + |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | + | + | + | + |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или | | | | |

| | | | | | |
|--|---|---|---|---|---|
| | переполнения объема (емкости) памяти | | | | |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них | | | + | + |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе | | | | |
| РСБ.7 | Защита информации о событиях безопасности | + | + | + | + |
| VI. Антивирусная защита (AB3) | | | | | |
| AB3.1 | Реализация антивирусной защиты | + | + | + | + |
| AB3.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | + | + | + | + |
| VII. Обнаружение вторжений (COB) | | | | | |
| COB.1 | Обнаружение вторжений | | | + | + |
| COB.2 | Обновление базы решающих правил | | | + | + |
| VIII. Контроль (анализ) защищенности персональных данных (АНЗ) | | | | | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей | | + | + | + |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | + | + | + | + |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | | + | + | + |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации | | + | + | + |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе | | | + | + |
| IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ) | | | | | |

| | | | | | |
|--|--|--|--|---|---|
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации | | | + | + |
| ОЦЛ.2 | Контроль целостности персональных данных, содержащихся в базах данных информационной системы | | | | |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций | | | | |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) | | | + | + |
| ОЦЛ.5 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы | | | | |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему | | | | |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему | | | | |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях | | | | |
| Х. Обеспечение доступности персональных данных (ОДТ) | | | | | |
| ОДТ.1 | Использование отказоустойчивых технических средств | | | | |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы | | | | |
| ОДТ.3 | Контроль безотказного функционирования | | | | + |

| | | | | | |
|--------------------------------------|---|---|---|---|---|
| | технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование | | | | |
| ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных | | | + | + |
| ОДТ.5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала | | | + | + |
| XI. Защита среды виртуализации (ЗСВ) | | | | | |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | + | + | + | + |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | + | + | + | + |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре | | + | + | + |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры | | | | |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией | | | | |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных | | | + | + |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигураций | | | + | + |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры | | | + | + |
| ЗСВ.9 | Реализация и управление антивирусной защитой в | | + | + | + |

| | | | | | |
|---|---|---|---|---|---|
| | виртуальной инфраструктуре | | | | |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей | | + | + | + |
| XII. Защита технических средств (ЗТС) | | | | | |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам | | | | |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования | | | | |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены | + | + | + | + |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | + | + | + | + |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) | | | | |
| XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС) | | | | | |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы | | | | + |

| | | | | | |
|-------|--|---|---|---|---|
| ЗИС.2 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом | | | | |
| ЗИС.3 | Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи | + | + | + | + |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) | | | | |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств | | | | |
| ЗИС.6 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами | | | | |
| ЗИС.7 | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода | | | | |
| ЗИС.8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи | | | | |
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации | | | | |

| | | | | | |
|---|---|--|---|---|---|
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам | | | | |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов | | | + | + |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю | | | | |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя | | | | |
| ЗИС.14 | Использование устройств терминального доступа для обработки персональных данных | | | | |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных | | | + | + |
| ЗИС.16 | Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов | | | | |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы | | | + | + |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения | | | | |
| ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти | | | | |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе | | + | + | + |
| XIV. Выявление инцидентов и реагирование на них (ИНЦ) | | | | | |
| ИНЦ.1 | Определение лиц, ответственных за выявление инцидентов и реагирование на них | | | + | + |

| | | | | | |
|--|---|--|---|---|---|
| ИНЦ.2 | Обнаружение, идентификация и регистрация инцидентов | | | + | + |
| ИНЦ.3 | Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами | | | + | + |
| ИНЦ.4 | Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий | | | + | + |
| ИНЦ.5 | Принятие мер по устранению последствий инцидентов | | | + | + |
| ИНЦ.6 | Планирование и принятие мер по предотвращению повторного возникновения инцидентов | | | + | + |
| XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ) | | | | | |
| УКФ.1 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных | | + | + | + |
| УКФ.2 | Управление изменениями конфигурации информационной системы и системы защиты персональных данных | | + | + | + |
| УКФ.3 | Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных | | + | + | + |
| УКФ.4 | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных | | + | + | + |

"+" - мера по обеспечению безопасности персональных данных включена в базовый набор мер для соответствующего уровня защищенности персональных данных.

Меры по обеспечению безопасности персональных данных, не обозначенные знаком "+", применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер по обеспечению безопасности персональных данных.