Анализ мер защиты для обеспечения 4 УЗ ПДн в ИСПДн.

Туманов И.А.

Постановление Правительства РФ №1119

12. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

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

A. 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;
B. обеспечение сохранности носителей персональных данных;
C. утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
D. 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.

Приказ ФСТЭК № 21

Для обеспечения 4 уровня защищенности персональных данных применяются:

- средства вычислительной техники не ниже 6 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса;
- межсетевые экраны 5 класса.

Состав мер защиты информации и их базовые наборы для 4 уровня защищенности:

- I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)
    - ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6.
- II. Управление доступом субъектов доступа к объектам доступа (УПД)
    - УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.13, УПД.14, УПД.15, УПД.16.
- V. Регистрация событий безопасности (РСБ)
    - РСБ.1, РСБ.2, РСБ.3, РСБ.7.
- VI. Антивирусная защита (АВЗ)
    - АВЗ.1, АВЗ.2.
- VIII. Контроль (анализ) защищенности персональных данных (АНЗ)
    - АНЗ.2.
- XI. Защита среды виртуализации (ЗСВ)
    - ЗСВ.1, ЗСВ.2.
- XII. Защита технических средств (ЗТС)
    - ЗТС.3, ЗТС.4
- XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)
    - ЗИС.3.

Расшифровка мер по методичке для 17 приказа

Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ).

ИАФ.1 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ
ПОЛЬЗОВАТЕЛЕЙ, ЯВЛЯЮЩИХСЯ РАБОТНИКАМИ ОПЕРАТОРА

Требования к реализации ИАФ.1: В информационной системе должна обеспечиваться идентификация и аутентификация пользователей, являющихся работниками оператора.
При доступе в информационную систему должна осуществляться идентификация и аутентификация пользователей, являющихся работниками оператора (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

!!! Доступ в ИСПДн только сотрудникам.
!!! Имена и пароли нужны и для ОС и для ИСПДн.

Требования к реализации ИАФ.3: Оператором должны быть установлены и реализованы следующие функции управления идентификаторами пользователей и устройств в информационной системе:

- определение должностного лица (администратора) оператора, ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств;
- формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;
- присвоение идентификатора пользователю и (или) устройству;
- предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установленного оператором периода времени;
- блокирование идентификатора пользователя после установленного оператором времени неиспользования.

Правила и процедуры управления идентификаторами регламентируются в организационно-распорядительных документах оператора по защите информации.

!!! Есть ответственное лицо за пароли.

Требования к реализации ИАФ.4: Оператором должны быть установлены и реализованы следующие функции управления средствами аутентификации

(аутентификационной информацией) пользователей и устройств в информационной системе:

- определение должностного лица (администратора) оператора, ответственного за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации информационной системы;
- выдача средств аутентификации пользователям;
- генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);
- установление характеристик пароля (при использовании в информационной системе механизмов аутентификации на основе пароля):

Требование к усилению ИАФ.4:
1) в случае использования в информационной системе механизмов аутентификации на основе пароля (иной последовательности символов, используемой для аутентификации) или применения пароля в качестве одного из факторов многофакторной аутентификации, его характеристики должны быть следующими:

а) длина пароля не менее шести символов, алфавит пароля не менее 30 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 3 до 15 минут, смена паролей не более чем через 180 дней;

!!! Журнал смены паролей?????
!!! Политика безопасности в домене

Требования к реализации ИАФ.5: В информационной системе должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.
Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками«*», «» или иными знаками.

Требования к реализации ИАФ.6: В информационной системе должна осуществляться однозначная идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей), или процессов, запускаемых от имени этих пользователей.
К пользователям, не являющимся работникам оператора (внешним пользователям), относятся все пользователи информационной системы, не указанные в ИАФ.1 в качестве внутренних пользователей. Примером внешних пользователей являются

граждане, на законных основаниях через сеть Интернет получающие доступ к информационным ресурсам портала Государственных услуг Российской Федерации «Электронного правительства» или официальным сайтам в сети Интернет органов государственной власти.

!!! ИАФ.6 к школам не относится.

ИТОГО:

1. Список сотрудников с логинами и паролями
2. Ответственное лицо за выдачу паролей
3. Пароль не короче 6 символов, смена не реже раза в 180 дней

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 УПРАВЛЕНИЯ ДОСТУПОМ (ДИСКРЕЦИОННЫЙ, МАНДАТНЫЙ, РОЛЕВОЙ ИЛИ ИНОЙ МЕТОД), ТИПОВ (ЧТЕНИЕ, ЗАПИСЬ, ВЫПОЛНЕНИЕ ИЛИ ИНОЙ ТИП) И ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА

Правила разграничения доступа реализуются на основе установленных оператором списков доступа или матриц доступа и должны обеспечивать управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам 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

Управление информационными потоками должно обеспечивать разрешенный установленный оператором) маршрут прохождения информации между пользователями, устройствами, сегментами в рамках информационной системы, а также между информационными системами или при взаимодействии с сетью Интернет(или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации информационной системы, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации). Управление информационными потоками должно блокировать передачу защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из информационной системы и (или) входящие в информационную систему.

!!! МЭ с прописанными правилами

УПД.4 РАЗДЕЛЕНИЕ ПОЛНОМОЧИЙ (РОЛЕЙ) ПОЛЬЗОВАТЕЛЕЙ, АДМИНИСТРАТОРОВ И ЛИЦ, ОБЕСПЕЧИВАЮЩИХ ФУНКЦИОНИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ.

см УПД.2

УПД.5 НАЗНАЧЕНИЕ МИНИМАЛЬНО НЕОБХОДИМЫХ ПРАВ И ПРИВИЛЕГИЙ ПОЛЬЗОВАТЕЛЯМ, АДМИНИСТРАТОРАМ И ЛИЦАМ, ОБЕСПЕЧИВАЮЩИМ ФУНКЦИОНИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ

см УПД.2

УПД.6 ОГРАНИЧЕНИЕ НЕУСПЕШНЫХ ПОПЫТОК ВХОДА В ИНФОРМАЦИОННУЮ СИСТЕМУ (ДОСТУПА К ИНФОРМАЦИОННОЙ СИСТЕМЕ)

Требования к реализации УПД.6: В информационной системе должно быть установлено и зафиксировано в организационно-распорядительных документах оператора по защите информации (задокументировано) ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за период времени, установленный оператором, а также обеспечено блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе).
Ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе)должно обеспечиваться в соответствии с ИАФ.4

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

предоставление беспроводного доступа в соответствии с УПД.2

УПД.15 РЕГЛАМЕНТАЦИЯ И КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ МОБИЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ

Требования к реализации УПД.15: Оператором должны обеспечиваться регламентация и контроль использования в информационной системе мобильных технических средств, направленные на защиту информации в информационной системе.
В качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и

иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства).
Регламентация и контроль использования мобильных технических средств должны включать:

- установление (в том числе документальное) видов доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа), разрешенных для доступа к объектам доступа информационной системы с использованием мобильных технических средств, входящих в состав информационной системы;
- использование в составе информационной системы для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации в соответствии с ЗИС.30;
- ограничение на использование мобильных технических средств в соответствии с задачами (функциями) информационной системы, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств в соответствии с УПД.2;
- мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа информационной системы;
- запрет возможности запуска без команды пользователя в информационной системе программного обеспечения (программного кода), используемого для взаимодействия с мобильным техническим средством.

Правила и процедуры применения мобильных технических средств, включая процедуры выдачи и возврата мобильных технических средств, а также их передачи на техническое обслуживание (процедура должна обеспечивать удаление или недоступность информации), регламентируются в организационно-распорядительных документах оператора по защите информации.

УПД.16 УПРАВЛЕНИЕ ВЗАИМОДЕЙСТВИЕМ С ИНФОРМАЦИОННЫМИ СИСТЕМАМИ СТОРОННИХ ОРГАНИЗАЦИЙ (ВНЕШНИЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ)

Требования к усилению УПД.16:
1) оператор предоставляет доступ к информационной системе авторизованным (уполномоченным) пользователям внешних информационных систем или разрешает обработку, хранение и передачу информации с использованием внешней информационной системы при выполнении следующих условий:

а) при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;

ИТОГО:

1. Матрица доступа пользователей, устройств и ПО.
2. МЭ с конкретными правилами пересылки трафика.
3. Запрет автозапуска ПО на мобильных технических средствах.

РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ (РСБ)

РСБ.1 ОПРЕДЕЛЕНИЕ СОБЫТИЙ БЕЗОПАСНОСТИ, ПОДЛЕЖАЩИХ РЕГИСТРАЦИИ, И СРОКОВ ИХ ХРАНЕНИЯ

В информационной системе как минимум подлежат регистрации следующие события:

- вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы;
- подключение машинных носителей информации и вывод информации на носители информации;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;
- попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;
- попытки удаленного доступа.

РСБ.2 ОПРЕДЕЛЕНИЕ СОСТАВА И СОДЕРЖАНИЯ ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ, ПОДЛЕЖАЩИХ РЕГИСТРАЦИИ

Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

РСБ.3 СБОР, ЗАПИСЬ И ХРАНЕНИЕ ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ В ТЕЧЕНИЕ УСТАНОВЛЕННОГО ВРЕМЕНИ ХРАНЕНИЯ

Требования к реализации РСБ.3: В информационной системе должны осуществляться сбор, запись и хранение информации о событиях безопасности в течение установленного оператором времени хранения информации о событиях безопасности.

РСБ.7 ЗАЩИТА ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ

Требования к реализации РСБ.7: В информационной системе должна обеспечиваться защита информации о событиях безопасности.

Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам.

ИТОГО:

1. Включаем и настраиваем журналирование и аудит в ОС

АНТИВИРУСНАЯ ЗАЩИТА (АВЗ)

АВЗ.1 РЕАЛИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ

Реализация антивирусной защиты должна предусматривать:

- применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), мобильных технических средствах и иных точках доступа в информационную систему, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы);
- установку, конфигурирование и управление средствами антивирусной защиты;
- предоставление доступа средствам антивирусной защиты к объектам информационной системы, которые должны быть подвергнуты проверке средством антивирусной защиты;
- проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов);
- проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов;
- оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);
- определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).

АВЗ.2 ОБНОВЛЕНИЕ БАЗЫ ДАННЫХ ПРИЗНАКОВ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ (ВИРУСОВ)

ИТОГО:

1. Антивирус должен быть везде, где возможно заражение
2. Должен быть именно монитор, а не сканер
3. Обновления регулярные обязательны
4. Оповещение администраторов - централизованная защита???

КОНТРОЛЬ (АНАЛИЗ) ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ (АН3)

АН3.1 ВЫЯВЛЕНИЕ, АНАЛИЗ И УСТРАНЕНИЕ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Требования к реализации АН3.1: Оператором должны осуществляться выявление (поиск), анализ и устранение уязвимостей в информационной системе.

В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей.

В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.
Оператором должны осуществляться получение из доверенных источников и установка обновлений базы признаков уязвимостей.

ИТОГО:

1. Регулярные обновления ПО и ОС.
2. Если для ОС не выходят обновления (windowsXP), то использовать можно, но с реализацией дополнительных мер защиты другими средствами.
3. http://bdu.fstec.ru !!!

ЗАЩИТА СРЕДЫ ВИРТУАЛИЗАЦИИ (ЗСВ)

ЗСВ.1 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ СУБЪЕКТОВ ДОСТУПА И ОБЪЕКТОВ ДОСТУПА В ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЕ, В ТОМ ЧИСЛЕ АДМИНИСТРАТОРОВ УПРАВЛЕНИЯ СРЕДСТВАМИ ВИРТУАЛИЗАЦИИ

Требования к реализации ЗСВ.1: В информационной системе должны обеспечиваться идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации, в соответствии с ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6 и ИАФ.7.

Внутри развернутых на базе виртуальной инфраструктуры виртуальных машин должна быть также обеспечена реализация мер по идентификации и аутентификации субъектов и объектов доступа в соответствии с ИАФ.1 – ИАФ.7.

ЗСВ.2 УПРАВЛЕНИЕ ДОСТУПОМ СУБЪЕКТОВ ДОСТУПА К ОБЪЕКТАМ ДОСТУПА В ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЕ, В ТОМ ЧИСЛЕ ВНУТРИ ВИРТУАЛЬНЫХ МАШИН

Требования к реализации ЗСВ.2: В информационной системе должно обеспечиваться управление доступом субъектов доступа к объектам доступа, в том числе внутри виртуальных машин, в соответствии с УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.9, УПД.10, УПД.11, УПД.12, УПД.13.

ЗАЩИТА ТЕХНИЧЕСКИХ СРЕДСТВ (ЗТС)

ЗТС.2 ОРГАНИЗАЦИЯ КОНТРОЛИРУЕМОЙ ЗОНЫ, В ПРЕДЕЛАХ КОТОРОЙ ПОСТОЯННО РАЗМЕЩАЮТСЯ СТАЦИОНАРНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА, ОБРАБАТЫВАЮЩИЕ ИНФОРМАЦИЮ, И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, А ТАКЖЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ФУНКЦИОНИРОВАНИЯ

Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) оператора и лиц, не имеющих постоянного допуска на объекты информационной системы (не являющихся работниками оператора), а также транспортных, технических и иных материальных средств.
Для одной информационной системы (ее сегментов) может быть организовано несколько контролируемых зон.

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 И ПОМЕЩЕНИЯ И СООРУЖЕНИЯ, В КОТОРЫХ ОНИ УСТАНОВЛЕНЫ

Контроль и управление физическим доступом должны предусматривать:

- определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
- санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
- учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

ЗТС.4 РАЗМЕЩЕНИЕ УСТРОЙСТВ ВЫВОДА (ОТОБРАЖЕНИЯ) ИНФОРМАЦИИ, ИСКЛЮЧАЮЩЕЕ ЕЕ НЕСАНКЦИОНИРОВАННЫЙ ПРОСМОТР

Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не следует размещать устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

ЗАЩИТА ИНФОРМАЦИОННОЙ СИСТЕМЫ, ЕЕ СРЕДСТВ И СИСТЕМ СВЯЗИ И ПЕРЕДАЧИ ДАННЫХ (ЗИС)

ЗИС.3 ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОТ РАСКРЫТИЯ, МОДИФИКАЦИИ И НАВЯЗЫВАНИЯ (ВВОДА ЛОЖНОЙ ИНФОРМАЦИИ) ПРИ ЕЕ ПЕРЕДАЧЕ (ПОДГОТОВКЕ К ПЕРЕДАЧЕ) ПО КАНАЛАМ СВЯЗИ, ИМЕЮЩИМ ВЫХОД ЗА ПРЕДЕЛЫ КОНТРОЛИРУЕМОЙ ЗОНЫ

Требования к реализации ЗИС.3: Оператором должна быть обеспечена защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны. Защита информации обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации или иными методами.

ИТОГОВЫЙ НАБОР МЕР

1. Список сотрудников с логинами и паролями
2. Ответственное лицо за выдачу паролей
3. Пароль не короче 6 символов, смена не реже раза в 180 дней
4. Матрица доступа пользователей, устройств и ПО.
5. МЭ с конкретными правилами пересылки трафика.
6. Запрет автозапуска ПО на мобильных технических средствах.
7. Включаем и настраиваем журналирование и аудит в ОС
8. Антивирус должен быть везде, где возможно заражение
9. Должен быть именно антивирусный монитор, а не сканер
10. Обновления антивируса регулярные обязательны
11. Оповещение администраторов - централизованная защита???
12. Регулярные обновления ПО и ОС.
13. Если для ОС не выходят обновления (WindowsXP), то использовать можно, но с реализацией дополнительных мер защиты другими средствами.
14. Определяем контролируемую зону