УТВЕРЖДАЮ:
Директор МОУ СОШ № 12
_____ И.А. Фоменко
«29» марта 2017 г.

Методы и способы защиты персональных данных от несанкционированного доступа в зависимости от класса информационной системы

Подсистемы и требования	К3	К2	К1
Для информационных систем при однопользовательском режиме обработки персональных данных			
Подсистема управления доступом:			
идентификация и проверка подлинности пользователя при входе в систему информационной системы по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов	+	+	+
Подсистема регистрации и учета			
регистрация входа (выхода) пользователя 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 информационной системы. В параметрах регистрации указываются:	+	+	+
– дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы	+	+	+
– результат попытки входа (успешная или неуспешная)	–	–	+
учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета	+	+	+
регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), краткое содержание документа (наименование, вид, код), спецификация устройства выдачи (логическое имя (номер) внешнего устройства)	–	–	+
дублирующий учет защищаемых носителей информации	–	–	+
очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних носителей информации	–	–	+
Подсистема обеспечения целостности			

Подсистема обеспечения целостности			
обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ	+	+	+
физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации	+	+	–
физическая охрана технических средств информационных систем (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания	–	–	+
периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа	+	+	+
наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности	+	+	+
Подсистема антивирусной защиты			
предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок	+	+	+
Подсистема защиты от утечки ПДн по ПЭМИН			
использование технических средств в защищенном исполнении	–	–	+
использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия	–	–	+
размещение объектов защиты в соответствии с предписанием на эксплуатацию	–	–	+
размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории	–	–	+
обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал	–	–	+
обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и	–	–	+

систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация			
Для информационных систем при многопользовательском режиме обработки персональных данных и равных правах доступа к ним пользователей			
Подсистема управления доступом:			
идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов	+	+	+
идентификация технических средств информационных систем и каналов связи, внешних устройств информационных систем по их логическим адресам (номерам)	–	–	+
идентификация программ, томов, каталогов, файлов, записей, полей записей по именам	–	–	+
Подсистема регистрации и учета			
регистрация входа (выхода) пользователя 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 информационной системы. <u>В параметрах регистрации указываются:</u>	+	+	+
– дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы	+	+	+
– результат попытки входа (успешная или неуспешная)	+	+	+
– идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа	–	–	+
учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета	+	+	–
учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме)	–	–	+
регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание документа (наименование, вид, шифр, код), идентификатор пользователя, запросившего документ	–	–	+
регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор пользователя, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный)	–	–	+
регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки	–	–	+

доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла			
регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер))	–	–	+
дублирующий учет защищаемых носителей информации	–	–	+
очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационных систем и внешних носителей информации	–	–	+
Подсистема обеспечения целостности			
обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации	+	+	+
физическая охрана информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации	+	+	–
физическая охрана технических средств информационной системы (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания	–	–	+
периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа	+	+	+
наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности	+	+	+
Подсистема антивирусной защиты			
предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок	+	+	+
Подсистема защиты от утечки ПДн по ПЭМИН			

использование технических средств в защищенном исполнении	–	–	+
использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия	–	–	+
размещение объектов защиты в соответствии с предписанием на эксплуатацию	–	–	+
размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории	–	–	+
обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал	–	–	+
обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация	–	–	+
Для информационных систем при многопользовательском режиме обработки персональных данных и разных правах доступа к ним пользователей			
Подсистема управления доступом:			
идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длинной не менее шести буквенно-цифровых символов	+	+	+
идентификация терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам	–	–	+
идентификация программ, томов, каталогов, файлов, записей, полей записей по именам	–	–	+
контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа	–	–	+
Подсистема регистрации и учета			
регистрация входа (выхода) пользователя 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 информационной системы. В параметрах регистрации указываются:	+	+	+
– дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы	+	+	+
– результат попытки входа (успешная или неуспешная)	+	+	+
– идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа	+	+	+
– код или пароль, предъявленный при неуспешной попытке	–	–	+
учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме)	+	+	+
регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер)	–	–	+

внешнего устройства), краткое содержание документа (наименование, вид, шифр, код), идентификатор пользователя, запросившего документ			
регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор пользователя, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный)	–	–	+
регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла	–	–	+
регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер))	–	–	+
очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних накопителей	–	–	+
Подсистема обеспечения целостности			
обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации	+	+	+
физическая охрана информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации	+	+	+
периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа	+	+	+
наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонент средств защиты информации,	+	+	+

их периодическое обновление и контроль работоспособности			
Подсистема антивирусной защиты			
предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок	+	+	+
Подсистема защиты от утечки ПДн по ПЭМИН			
использование технических средств в защищенном исполнении	–	–	+
использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия	–	–	+
размещение объектов защиты в соответствии с предписанием на эксплуатацию	–	–	+
размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории	–	–	+
обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал	–	–	+
обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация	–	–	+
Подсистема обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений для информационных систем К3 при их подключении к сетям международного информационного обмена, а также для распределенных информационных систем классов К1, К2, К3 при их разделении на подсистемы			
фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов)			
идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия			
регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана)			
контроль целостности своей программной и информационной части			
фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств			
восстановление свойств межсетевого экрана после сбоев и отказов оборудования			
регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления			
создание канала связи, обеспечивающего защиту передаваемой информации			
Подсистема обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений для информационных систем К2 при их подключении к сетям международного информационного обмена			
фильтрацию на сетевом уровне независимо для каждого сетевого пакета (решение о			

фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов)
фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств
фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов
фильтрацию с учетом любых значимых полей сетевых пакетов
регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации)
идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия
регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана)
регистрацию запуска программ и процессов (заданий, задач)
контроль целостности своей программной и информационной части
восстановление свойств межсетевого экрана после сбоев и отказов оборудования
регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления
создание канала связи, обеспечивающего защиту передаваемой информации
Подсистема обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений для информационных систем **К1** при их подключении к сетям международного информационного обмена
фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов)
фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств
фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов
фильтрацию с учетом любых значимых полей сетевых пакетов
фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя
фильтрацию на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя
фильтрацию с учетом даты и времени
аутентификацию входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети
регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации)
регистрацию и учет запросов на установление виртуальных соединений
локальную сигнализацию попыток нарушения правил фильтрации
идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия
предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась
идентификацию и аутентификацию администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации
регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы)

либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана)	
регистрацию запуска программ и процессов (заданий, задач)	
регистрацию действия администратора межсетевого экрана по изменению правил фильтрации	
возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации	
контроль целостности своей программной и информационной части	
контроль целостности программной и информационной части межсетевого экрана по контрольным суммам	
восстановление свойств межсетевого экрана после сбоев и отказов оборудования	
регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления	
создание канала связи, обеспечивающего защиту передаваемой информации	
Подсистема анализа защищенности	
Анализ защищенности **проводится для распределенных информационных систем и информационных систем, подключенных к сетям международного информационного обмена**, путем использования в составе информационной системы программных или программно-аппаратных средств (систем) анализа защищенности. Средства (системы) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему	
Подсистема обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений	
Обнаружение вторжений проводится **для информационных систем, подключенных к сетям международного информационного обмена**, путем использования в составе информационной системы программных или программно-аппаратных средств (систем) обнаружения вторжений	