Приложение № 2
к приказу МБОУ гимназии № 103
г. Минеральные Воды
от «14» февраля 2023 г. № 69

Модель угроз безопасности
информационной системы по обработке персональных данных
(ИСПДн) МБОУ гимназии № 103 г. Минеральные Воды

При разработке модели угроз ИСПДн необходимо:

- определить источники УБИ;
- определить способы реализации угроз безопасности информации;
- оценить актуальность угроз безопасности информации в информационной системе;
- определить меры защиты информации в ИСПДн.

Для определения набора актуальных угроз безопасности информации для ранее спроектированной ИСПДн необходимо опираться на:

– характеристики рассматриваемой ИСПДн;

– общий перечень УБИ, содержащийся в банке данных УБИ ФСТЭК России, размещённом в информационно-телекоммуникационной сети «Интернет» по адресу bdu.fstec.ru (далее – БД УБИ);

– методический документ ФСТЭК России «Методика оценки угроз безопасности информации», утверждённый 5 февраля 2021 года (далее – Методика).

Для определения актуальных УБИ для рассматриваемой ИСПДн необходимо использовать алгоритм, описанный в пятой главе Методики («Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности»).

Для выполнения объявленного алгоритма необходимо выполнить следующие действия:

1. Определение видов актуальных нарушителей, возможных целей реализации ими угроз безопасности информации, их возможностей (приложения 6-9 Методики).

2. Определение актуальных способов реализации угроз безопасности информации и соответствующих им видов актуальных нарушителей и их возможностей (приложение 10 Методики).

3. Определение тактик и техник реализации угроз безопасности информации, которые могут быть использовать актуальным нарушителями в рамках актуальных способов реализации угроз безопасности информации (приложение 11 Методики).

4. Определение актуальности УБИ из БД УБИ в соответствии с хотя бы одной из определённых тактик и формирование перечня актуальных для ИСПДн угроз.

Методика выделяет следующие виды нарушителей:

– специальные службы иностранных государств;

– террористические, экстремистские группировки;

– преступные группы (криминальные структуры);

– отдельные физические лица (хакеры);

– разработчики программных, программно-аппаратных средств;

– лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;

– поставщики услуг связи, вычислительных услуг;

– лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;

– лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.);

– авторизованные пользователи систем и сетей;

– системные администраторы и администраторы безопасности;

– бывшие (уволенные) работники (пользователи).

В зависимости от видов актуальных нарушителей для рассматриваемой ИСПДн будут актуальны разные способы реализации УБИ, применяемые техники и тактики и, соответственно, актуальные УБИ.

На основе выписки «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России, 2008 год, установим возможные угрозы.

При обработке ПДн в локальных ИСПДн, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих УБПДн:

- угрозы утечки информации по техническим каналам;
- угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте.

Угрозы утечки информации по техническим каналам включают в себя:

- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.

Угрозы из внешних сетей включают в себя:

- угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа операционной системы ИСПДн, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей;
- угрозы получения НСД путем подмены доверенного объекта;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

В таблице 1.1 приведены виды актуальных нарушителей и их возможные цели реализации УБИ по отношению к рассматриваемой ИСПДн.

Таблица 1.1

Виды актуальных нарушителей и их характеристика

№ п/п	Вид нарушителя	Цели реализации УБИ	Возможности нарушителя
1	Отдельные физические лица (хакеры)	Получение выгоды за счёт персональных данных	Использование известных уязвимостей и/или инструментов, в том числе свободно распространяемых в сети «Интернет»
2	Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора	1) Непреднамеренная реализация УБИ 2) Получение финансовой или иной выгоды 3) Месть за ранее совершённые действия	1) Использование известных уязвимостей и/или инструментов; 2) Физическое воздействие на объекты информационной инфраструктуры
3	Авторизованные пользователи систем и сетей	1) Непреднамеренная реализация УБИ 3) Получение финансовой или иной выгоды	Использование известных уязвимостей и/или инструментов, в том числе свободно распространяемых в сети «Интернет»
4	Системные администраторы и администраторы безопасности	1) Непреднамеренная реализация УБИ 2) Получение финансовой или иной выгоды 2) Месть за ранее совершённые действия	1) Использование известных уязвимостей и/или инструментов, в том числе свободно распространяемых в сети «Интернет»; 2) Физическое воздействие на объекты информационной инфраструктуры; 3) Реализация УБИ, направленных на неизвестные (недокументиро-

			ванные) уязвимости
5	Бывшие (уволенные) работники (пользователи)	3) Месть за ранее совершённые действия	Использование известных уязвимостей и/или инструментов, в том числе свободно распространяемых в сети «Интернет»

Следующим действием является рассмотрение актуальных способов реализации УБИ актуальными нарушителями для ИСДПн согласно приложению 10 Методики. В таблице 1.2 представлены актуальные способы реализации УБИ по отношению к рассматриваемой ИСПДн.

Таблица 1.2

Актуальные способы реализации УБИ

№ п/п	Вид нарушителя	Способ реализации УБИ
1	Отдельные физические лица (хакеры)	1) Внедрение вредоносного программного обеспечения 2) Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя 3) Использование уязвимостей кода программного обеспечения веб-сервера 4) Внедрение вредоносного кода в веб-приложение
2	Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора	1) Установка закладок 2) Физический доступ к объектам информационной инфраструктуры и воздействие на них
3	Авторизованные пользователи систем и сетей	1) Ошибочные действия в процессе работы с системой 2) Внедрение вредоносного программного обеспечения 3) Использование уязвимостей кода программного обеспечения веб-сервера 4) Внедрение вредоносного кода в веб-приложение
4	Системные администраторы и администраторы безопасности	1) Установка закладок 2) Физический доступ к объектам информационной инфраструктуры и воздействие на них 3) Доступ к АРМ сотрудников, серверам или телекоммуникационному оборудованию под видом исполнения собственных полномочий 4) Внедрение вредоносного программного обеспечения 5) Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя 6) Использование уязвимостей кода программного обеспечения веб-сервера 7) Внедрение вредоносного кода в веб-приложение
5	Бывшие (уволенные) работники (пользователи)	1) Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя 2) Использование уязвимостей кода программного обеспечения веб-сервера

Следующим действием является определение и документирование основных техник и типовых тактик, при помощи которых становится возможным построение и реализация сценария реализации УБИ актуальными способами.

В таблице 1.3 представлены выявленные основные техники и типовые атаки, которые имеют возможность реализации по отношению к рассматриваемой ИСДПн.

Таблица 1.3

Основные тактики и типовые техники, используемые для построения сценариев реализации УБИ актуальными способами

№	Тактика	Техники
Т1	Сбор информации о системах и сетях	Т1.1. Сбор информации из публичных источников; Т1.2. Сбор информации о подключенных к публичным сис-

		темам и сетям устройствах и их службах при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений; Т1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях – идентификационной информации пользователей; Т1.4. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений; Т1.5. Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств; Т1.8. Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера; Т1.20. Техники конкурентной разведки и промышленного шпионажа для сбора информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами
Т2	Получение первоначального доступа к компонентам систем и сетей	Т2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет); Т2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке; Т2.4. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке; Т2.5. Эксплуатация уязвимостей компонентов систем и сетей при удаленной или локальной атаке; Т2.6. Использование недокументированных возможностей программного обеспечения сервисов, приложений, оборудования, включая использование отладочных интерфейсов, программных, программно-аппаратных закладок; Т2.7. Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением; Т2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы; Т2.9. Несанкционированное подключение внешних устройств; Т2.10. Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя

Т3	Внедрение и исполнение вредоносного программного обеспечения в системах и сетях	Т3.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии; Т3.2. Активация и выполнение вредоносного кода, внедренного в виде закладок в легитимное программное и программное-аппаратное обеспечение систем и сетей; Т3.3. Автоматическая загрузка вредоносного кода с удаленного сайта или ресурса с последующим запуском на выполнение; Т3.6. Автоматическое создание вредоносных скриптов при помощи доступного инструментария от имени пользователя в системе с использованием его учетных данных; Т3.14. Планирование запуска вредоносных программ при старте операционной системы путем эксплуатации стандартных механизмов, в том числе путем правки ключей реестра, отвечающих за автоматический запуск программ, запуска вредоносных программ как сервисов и т.п.
Т4	Закрепление (сохранение доступа) в системе или сети	Т4.1. Несанкционированное создание учетных записей или кража существующих учетных данных; Т4.2. Использование штатных средств удаленного доступа и управления операционной системы; Т4.3. Скрытая установка и запуск средств удаленного доступа и управления операционной системы; Т4.4. Маскирование подключенных устройств под легитимные (например, нанесение корпоративного логотипа, инвентарного номера, телефона службы поддержки); Т4.5. Внесение соответствующих записей в реестр, автозагрузку, планировщики заданий, обеспечивающих запуск вредоносного программного обеспечения при перезагрузке системы или сети; Т4.6. Компрометация прошивок устройств с использованием уязвимостей или программно-аппаратных закладок, к примеру, внедрение новых функций в BIOS (UEFI), компрометация прошивок жестких дисков
Т5	Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ	Т5.1. Удаленное управление через стандартные протоколы (например, RDP, SSH), а также использование инфраструктуры провайдеров, средств удаленного администрирования; Т5.2. Использование штатных средств удаленного доступа и управления операционной системы; Т5.3. Коммуникация с внешними серверами управления через хорошо известные порты на этих серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.); Т5.4. Коммуникация с внешними серверами управления через нестандартные порты на этих серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств; Т5.6. Проксирование трафика управления для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика управления во избежание обнаружения; Т5.12. Передача команд управления через публикацию на внешнем легитимном сервисе, таком как веб-сайт, облачный ресурс, ресурс в социальной сети и т.п.

Т6	Повышение привилегий по доступу к компонентам систем и сетей	Т6.1. Получение данных для аутентификации и авторизации от имени привилегированной учетной записи путем поиска этих данных в папках и файлах, поиска в памяти или перехвата в сетевом трафике; Т6.2. Подбор пароля или другой информации для аутентификации от имени привилегированной учетной записи; Т6.3 Эксплуатация уязвимостей ПО к повышению привилегий; Т6.4. Эксплуатация уязвимостей механизма имперсонации (запуска операций в системе от имени другой учетной записи); Т6.5. Манипуляции с идентификатором сессии, токеном доступа или иным параметром, определяющим права и полномочия пользователя в системе таким образом, что новый или измененный идентификатор/токен/параметр дает возможность выполнения ранее недоступных пользователю операций; Т6.6. Обход политики ограничения пользовательских учетных записей в выполнении групп операций, требующих привилегированного режима; Т6.7. Использование уязвимостей конфигурации системы, служб и приложений; Т6.8. Эксплуатация уязвимостей, связанных с отдельным, и вероятно менее строгим контролем доступа к некоторым ресурсам (например, к файловой системе) для непривилегированных учетных записей
Т7	Сокрытие действий и применяемых при этом средств от обнаружения	Т7.1. Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения; Т7.2. Очистка/затирание истории команд и журналов регистрации, перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей; Т7.3. Удаление файлов, переписывание файлов произвольными данными, форматирование съемных носителей; Т7.4. Отключение средств защиты от угроз информационной безопасности, в том числе средств антивирусной защиты, механизмов аудита, консолей оператора мониторинга и средств защиты других типов; Т7.6. Подделка данных вывода средств защиты от угроз информационной безопасности; Т7.8. Выполнение атаки отказа в обслуживании на основные и резервные каналы связи, которые могут использоваться для доставки сообщений о неработоспособности систем или их компонентов или о других признаках атаки; Т7.10. Внедрение вредоносного кода в доверенные процессы операционной системы и другие объекты, которые не подвергаются анализу на наличие такого кода, для предотвращения обнаружения; Т7.11. Модификация модулей и конфигурации вредоносного программного обеспечения для затруднения его обнаружения в системе; Т7.12. Манипуляции именами и параметрами запуска процессов и приложений для обеспечения скрытности;

		Т7.13. Создание скрытых файлов, скрытых учетных записей; Т7.16. Искусственное временное ограничение распространения или активации вредоносного кода внутри сети, во избежание преждевременного обнаружения факта атаки; Т7.17. Обфускация, шифрование, упаковка с защитой паролем или сокрытие стеганографическими методами программного кода вредоносного ПО, данных и команд управляющего трафика, в том числе при хранении этого кода и данных в атакуемой системе, при хранении на сетевом ресурсе или при передаче по сети; Т7.21. Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами; Т7.22. Подмена и компрометация прошивок, в том числе прошивок BIOS, жестких дисков; Т7.23. Подмена файлов легитимных программ и библиотек непосредственно в системе
Т8	Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям	Т8.1. Эксплуатация уязвимостей для повышения привилегий в системе или сети для удаленного выполнения программного кода для распространения доступа; Т8.2. Использование средств и интерфейсов удаленного управления для получения доступа к смежным системам и сетям; Т8.3. Использование механизмов дистанционной установки программного обеспечения и конфигурирования; Т8.4. Удаленное копирование файлов, включая модули вредоносного программного обеспечения и легитимные программные средства, которые позволяют злоумышленнику получать доступ к смежным системам и сетям; Т8.5. Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами; Т8.6. Копирование вредоносного кода на съемные носители; Т8.7. Размещение вредоносных программных модулей на разделяемых сетевых ресурсах в сети
Т9	Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз	Т9.1. Доступ к системе для сбора информации и вывод информации через стандартные протоколы управления (например, RDP, SSH), а также использование инфраструктуры провайдеров, средств удаленного администрирования; Т9.2. Доступ к системе для сбора информации и вывод информации через использование штатных средств удаленного доступа и управления операционной системы; Т9.3. Вывод информации на хорошо известные порты на внешних серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.); Т9.4. Вывод информации на нестандартные порты на внешних серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств; Т9.5. Отправка данных по известным протоколам управления и передачи данных Т9.6. Отправка данных по собственным протоколам;

		Т9.7. Проксирование трафика передачи данных для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика передачи данных во избежание обнаружения; Т9.12. Шифрование выводимой информации, использование стеганографии для сокрытия факта вывода информации; Т9.13. Вывод информации через предоставление доступа к файловым хранилищам и базам данных в инфраструктуре скомпрометированной системы или сети, в том числе путем создания новых учетных записей или передачи данных для аутентификации и авторизации имеющихся учетных записей; Т9.14. Вывод информации путем размещения сообщений или файлов на публичных ресурсах, доступных для анонимного нарушителя (форумы, файлообменные сервисы, фотобанки, облачные сервисы, социальные сети)
Т10	Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям	Т10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках; Т10.2. Несанкционированное воздействие на системное программное обеспечение, его конфигурацию и параметры доступа; Т10.3. Несанкционированное воздействие на программные модули прикладного программного обеспечения; Т10.4. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прикладного программного обеспечения; Т10.5. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа системного программного обеспечения; Т10.7. Подмена информации в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей; Т10.8. Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей; Т10.9. Добавление информации (например, дефейсинг корпоративного портала, публикация ложной новости); Т10.10. Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети; Т10.11. Нецелевое использование ресурсов системы

После определения всех видов актуальных нарушителей, их характеристик, возможностей, используемых ими способов, техник и тактик реализации УБИ становится возможным проанализировать БД УБИ и определить список актуальных УБИ для рассматриваемой ИСПДн согласно изложенному ранее алгоритму.

В таблице 1.4 описаны УБИ, актуальные для рассматриваемой ИСПДн.

Таблица 1.4

Актуальные УБИ для ИСПДн МБОУ гимназии № 103 г. Минеральные Воды

№ п/п	Идентификатор угрозы в БД УБИ	Название УБИ
1	УБИ.004	Угроза аппаратного сброса пароля BIOS
2	УБИ.005	Угроза внедрения вредоносного кода в BIOS
3	УБИ.006	Угроза внедрения кода или данных
4	УБИ.007	Угроза воздействия на программы с высокими привилегиями
5	УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации
6	УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ
7	УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями
8	УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути
9	УБИ.016	Угроза доступа к локальным файлам сервера при помощи URL
10	УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies
11	УБИ.018	Угроза загрузки нештатной операционной системы
12	УБИ.022	Угроза избыточного выделения оперативной памяти
13	УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы
14	УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
15	УБИ.036	Угроза исследования механизмов работы программы
16	УБИ.037	Угроза исследования приложения через отчёты об ошибках
17	УБИ.041	Угроза межсайтового скриптинга
18	УБИ.042	Угроза межсайтовой подделки запроса
19	УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией
20	УБИ.074	Угроза несанкционированного доступа к аутентификационной информации
21	УБИ.091	Угроза несанкционированного удаления защищаемой информации
22	УБИ.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам
23	УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб
24	УБИ.099	Угроза обнаружения хостов
25	УБИ.103	Угроза определения типов объектов защиты
26	УБИ.104	Угроза определения топологии вычислительной сети
27	УБИ.112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением
28	УБИ.114	Угроза переполнения целочисленных переменных
29	УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
30	УБИ.122	Угроза повышения привилегий
31	УБИ.127	Угроза подмены действия пользователя путём обмана
32	УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
33	УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
34	УБИ.159	Угроза «форсированного веб-браузинга»
35	УБИ.169	Угроза наличия механизмов разработчика
36	УБИ.173	Угроза «спама» веб-сервера
37	УБИ.179	Угроза несанкционированной модификации защищаемой информации
38	УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения
39	УБИ.192	Угроза использования уязвимых версий программного обеспечения
40	УБИ.195	Угроза удаленного запуска вредоносного кода в обход механизмов защи-

		ты операционной системы
41	УБИ.197	Угроза хищения аутентификационной информации из временных файлов cookie
42	УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты
43	УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники
44	УБИ 209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
45	УБИ 210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения
46	УБИ 212	Угроза перехвата управления информационной системой
47	УБИ 214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации
48	УБИ 215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов
49	УБИ 217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения

Таким образом, в результате выполнения алгоритма, описанного в главе 5 Методики, был получен список УБИ, актуальных для реализации по отношению к рассматриваемой ИСПДн. Полученные список можно использовать для формирования наборов мер защиты от реализации УБИ.

Далее необходимо выделить базовый набор мер, руководствуясь приложением к Приказу ФСТЭК №21 и учитывая факт необходимости обеспечения третьего уровня защищённости ПДн. Полученный базовый набор мер представлен в таблице 1.5.

Таблица 1.5

Базовый набор мер защиты ПДн

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
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
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.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.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
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.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
XII. Защита технических средств (ЗТС)	
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
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
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.20	Защита беспроводных соединений, применяемых в информационной системе
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

Данный базовый набор мер позволит избавиться или уменьшить риск возможных угроз, приведенных в таблице 1.4. В случае, если базового набора мер защиты информации окажется недостаточно для блокирования УБИ, в таблице 1.6 приведен уточненный базовый список мер, в который включены меры защиты информации, позволяющие заблокировать все УБИ.

Таблица 1.6

Уточнённый базовый список мер защиты ПДн

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
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
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.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)
III. Ограничение программной среды (ОПС)	
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.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.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах
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.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
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.4	Контроль состава технических средств, программного обеспечения и средств защиты

	информации
XII. Защита технических средств (ЗТС)	
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам
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.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.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе
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