|  |  |
| --- | --- |
|  |  |
|  |
|  |

Общий порядок определения мер по обеспечению безопасности информации для их реализации в сегменте ГИС представлен на рисунке 1.



Рисунок 1 – Общий порядок определения мер по обеспечению безопасности информации для их реализации в сегменте ГИС

1.2 При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности информации, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться компенсирующие меры, направленные на нейтрализацию актуальных угроз безопасности информации.

2. Определение базового набора мер по обеспечению безопасности информации

Для установленного 3-го класса защищенности сегмента ГИС, в базовый набор включены следующие меры:

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;

ИАФ.6 Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей);

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.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.13 Реализация защищенного удаленного 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);

ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;

ЗНИ.1 Учет машинных носителей информации;

ЗНИ.2 Управление доступом к машинным носителям информации;

ЗНИ.8 Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания);

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 течении 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;

АВЗ.1 Реализация антивирусной защиты;

АВЗ.2 Обновление баз данных признаков вредоносных компьютерных программ (вирусов);

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;

ОЦЛ.3 Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций;

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.9 Реализация и управление антивирусной защитой в виртуальной инфраструктуре;

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;

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, в том числе беспроводным каналам связи;

ЗИС.5 Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств;

ЗИС.20 Защита беспроводных соединений, применяемых в информационной системе;

ЗИС.30 Защита мобильных технических средств, применяемых в информационной системе.

3. Адаптация базового набора мер по обеспечению безопасности информации

3.1 В сегменте ГИС «ЕИС ГМУ СО» не используются следующие технологии:

– беспроводной доступ;

– использование мобильных технических средств;

– использование технологий удаленного доступа;

– использование виртуализации.

3.2 С учетом структурно-функциональных характеристик, информационных технологий и особенностей функционирования сегмента ГИС из базового набора мер для 3-го класса защищенности сегмента ГИС исключаются следующие меры:

ИАФ.6 Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей);

УПД.13 Реализация защищенного удаленного 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;

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.9 Реализация и управление антивирусной защитой в виртуальной инфраструктуре;

ЗИС.5 Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств;

ЗИС.20 Защита беспроводных соединений, применяемых в информационной системе;

ЗИС.30 Защита мобильных технических средств, применяемых в информационной системе.

4. Уточнение адаптированного базового набора мер по обеспечению безопасности информации

4.1 Помимо выбранных на предыдущих этапах мер для нейтрализации актуальных угроз безопасности информации, включенных в Модель угроз безопасности информации при их обработке в сегменте ГИС «ЕИС ГМУ СО», необходимо дополнительно реализовать следующие меры:

УПД.З Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами.

Соответствие актуальных угроз безопасности информации и мер по обеспечению информационной безопасности представлено в таблице 1.

Таблица 1 – Соответствие актуальных угроз безопасности информации и мер по обеспечению информационной безопасности

| № п/п | Угроза | Мера |
| --- | --- | --- |
| 1. Угрозы непосредственного доступа в операционную среду (ОС) |
| 1.1 | Угроза, реализуемая до загрузки ОС | УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;АНЗ.4 Контроль состава технических средств, программного обеспечения и средств защиты информации;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; |
| 1.2 | Угроза, реализуемая после загрузки ОС | ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора;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.10 Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;ЗНИ.2 Управление доступом к машинным носителям информации;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 течении установленного времени хранения;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;АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;ЗТС.4 Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр; |
| 1.3 | Угроза компрометации парольной информации | 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;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;ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;ЗНИ.2 Управление доступом к машинным носителям информации;ЗНИ.8 Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания);РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения;РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;АВЗ.1 Реализация антивирусной защиты;АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе;ЗТС.4 Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;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, в том числе беспроводным каналам связи; |
| 2. Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия |
| 2.1 | Анализ сетевого трафика | 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, в том числе беспроводным каналам связи;УПД.З Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами. |
| 2.2 | Сканирование сети | УПД.З Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами. |
| 2.3 | Удаленный запуск приложений через распространение файлов, содержащих несанкционированный исполняемый код | УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;АВЗ.1 Реализация антивирусной защиты;АВЗ.2 Обновление баз данных признаков вредоносных компьютерных программ (вирусов); |
| 2.4 | Удаленный запуск приложений путем переполнения буферов приложений | УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;АВЗ.1 Реализация антивирусной защиты;АВЗ.2 Обновление баз данных признаков вредоносных компьютерных программ (вирусов); |
| 2.5 | Удаленный запуск приложений путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами | УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;АВЗ.1 Реализация антивирусной защиты;АВЗ.2 Обновление баз данных признаков вредоносных компьютерных программ (вирусов);УПД.З Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами. |
| 3. Угрозы внедрения вредоносных программ (программно-математических воздействий) |
| 3.1 | Файловые вирусы | ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;АВЗ.1 Реализация антивирусной защиты;АВЗ.2 Обновление баз данных признаков вредоносных компьютерных программ (вирусов); |
| 3.2 | Загрузочные вирусы |
| 3.3 | Сетевые вирусы (сетевые черви) |
| 3.4 | Троянские программы |

5. Дополнение уточненного адаптированного базового набора мер по обеспечению безопасности информации

5.1 Уточненный адаптированный базовый набор мер по обеспечению безопасности информации дополняется мерами, обеспечивающими выполнение требований к защите персональных данных, установленными Постановлением Правительства РФ № 1119 от 1 ноября 2012 г.
«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»:

– 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;

– обеспечение сохранности носителей персональных данных;

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

– 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;

– назначение руководителем оператора должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

5.2 Таким образом, дополненный уточненный адаптированный базовый набор мер по обеспечению безопасности ПДн включает в себя следующие меры:

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;

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.З 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.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.16 Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы);

ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;

ЗНИ.1 Учет машинных носителей информации;

ЗНИ.2 Управление доступом к машинным носителям информации;

ЗНИ.8 Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания);

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 течении 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;

АВЗ.1 Реализация антивирусной защиты;

АВЗ.2 Обновление баз данных признаков вредоносных компьютерных программ (вирусов);

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;

ОЦЛ.3 Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций;

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;

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, в том числе беспроводным каналам связи;

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;

Обеспечение сохранности носителей персональных данных;

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

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;

Назначение руководителем оператора должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

|  |  |
| --- | --- |
| Секретарь руководителя | Л. Ю. Шавкута |