Государственное автономное учреждение
дополнительного профессионального образования
«Смоленский областной институт развития образования»
(ГАУ ДПО СОИРО)

ПРИКАЗ

21.10.2024 № 201-09

О реализации мер по защите информации в информационных системах ГАУ ДПО «Смоленский областной институт развития образования»

В целях защиты информации, не составляющей государственную тайну, и персональных данных, содержащихся в информационных системах ГАУ ДПО «Смоленский областной институт развития образования», и выполнения требований приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»,

п р и к а з ы в а ю :

1. Утвердить нижеследующие внутренние документы ГАУ ДПО «Смоленский областной институт развития образования»:

– Регламент идентификации и аутентификации в информационных системах ГАУ ДПО «Смоленский областной институт развития образования» (Приложение № 1);

– Регламент управления доступом в информационных системах ГАУ ДПО «Смоленский областной институт развития образования» (Приложение № 2);

– Регламент ограничения программной среды в информационных системах ГАУ ДПО «Смоленский областной институт развития образования» (Приложение № 3);

– Регламент защиты машинных носителей в информационных системах ГАУ ДПО «Смоленский областной институт развития образования» (Приложение № 4);

– Регламент регистрации событий безопасности в информационных системах ГАУ ДПО «Смоленский областной институт развития образования» (Приложение № 5);

– Регламент антивирусной защиты информационных систем ГАУ ДПО «Смоленский областной институт развития образования» (Приложение № 6);

– Регламент обнаружения вторжений в информационных системах ГАУ ДПО «Смоленский областной институт развития образования» (Приложение № 7);

– Регламент контроля (анализа) защищенности информации в информационных системах ГАУ ДПО «Смоленский областной институт развития образования» (Приложение № 8);

– Регламент обеспечения целостности информационных систем ГАУ ДПО «Смоленский областной институт развития образования» (Приложение № 9);

– Регламент обеспечения доступности информационных систем ГАУ ДПО «Смоленский областной институт развития образования» (Приложение № 10);

– Регламент защиты среды виртуализации в информационных системах ГАУ ДПО «Смоленский областной институт развития образования» (Приложение № 11);

– Регламент защиты технических средств в информационных системах ГАУ ДПО «Смоленский областной институт развития образования» (Приложение № 12);

– Регламент защиты информационных систем ГАУ ДПО «Смоленский областной институт развития образования», их средств, систем связи и передачи данных (Приложение № 13).

2. Контроль за исполнением настоящего приказа оставляю за собой.

И.о. ректора **С.П. Захаров**

Приложение № 1
к приказу ГАУ ДПО «Смоленский областной
институт развития образования»
от «21» 10 2024г. №201-09

Регламент идентификации и аутентификации в информационных системах ГАУ ДПО «Смоленский областной институт развития образования»

1. Общие положения

1.1. Настоящий Регламент разработан с целью установления ГАУ ДПО «Смоленский областной институт развития образования» (далее – Институт) общих правил, требований и процедур идентификации и аутентификации при разработке, внедрении и совершенствовании правил, механизмов и технологий управления доступом к информационным системам (далее – ИС) Института.

1.2. Меры защиты информации, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты информации, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты информации
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

1.3. Состав мер определен на основании установленного класса защищенности информационной системы, уровня защищенности персональных данных и структурно-функциональных характеристик ИС Института.

1.4. Регламент предназначен для сотрудников Института:

1.4.1. Назначенных ответственными за обеспечение безопасности персональных данных.

1.4.2. Назначенных ответственными за защиту информации.

1.4.3. Выполняющих функции по управлению (администрированию) системой защиты информации.

1.4.4. Выполняющих функции по управлению конфигурацией информационной системы и ее системы защиты информации.

2. Термины и определения

2.1. Аутентификационная информация (информация аутентификации) – информация, используемая для установления подлинности (верификации) субъекта доступа в информационной (автоматизированной) системе.

2.2. Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной (автоматизированной) системе).

2.3. Идентификатор доступа (идентификатор) – уникальный признак субъекта или объекта доступа (представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной (автоматизированной) системе).

2.4. Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

2.5. Несанкционированный доступ (НСД) – доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа.

2.6. Объект доступа – единица информационного ресурса информационной (автоматизированной) системы (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции.

2.7. Пароль – Идентификатор субъекта доступа, который является его (субъекта) секретом.

2.8. Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной (автоматизированной) системе или использующее результаты ее функционирования.

2.9. Субъект доступа – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

2.10. Управление доступом – ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа.

3. Цель и задачи реализации процессов идентификации и аутентификации

3.1. Целью реализации процессов идентификации и аутентификации в ИС Института является распознавание субъекта доступа с необходимой уверенностью в том, что он является именно тем, за кого себя выдает.

3.2. Реализация процессов идентификации и аутентификации достигается решением следующих задач:

– формированием и регистрацией информации о субъекте (объекте) доступа, а также присвоением субъекту (объекту) доступа идентификатора доступа и его регистрацией в перечне присвоенных идентификаторов;

– хранением и поддержанием в актуальном состоянии (обновлением) идентификационной и аутентификационной информации субъекта (объекта) доступа в соответствии с установленными правилами;

– опознаванием субъекта доступа, запросившего доступ к объекту доступа, по предъявленному идентификатору;

– аутентификацией, включающей проверку подлинности субъекта (объекта) доступа и принадлежности ему предъявленных идентификатора и аутентификационной информации.

4. Общие требования

4.1. Процессы идентификации и аутентификации в ИС Института подлежат реализации при управлении доступом к:

– СУБД PostgreSQL

– СУБД MySQL

4.2. Идентификация и аутентификация должна осуществляться в отношении:

– пользователей ИС Института, являющихся сотрудниками Института;

– пользователей ИС Института, не являющихся сотрудниками Института;

– процессов, запускаемых от имени пользователей;

– процессов, запускаемых от имени системных учетных записей;

– устройств (технических средств), участвующих в информационном взаимодействии.

4.3. Процессы, запускаемые от имени пользователя, должны однозначно сопоставляться с идентификатором пользователя.

4.4. В качестве идентификатора пользователя при доступе должен использоваться набор буквенно-цифровых символов (логин).

4.5. В ИС Института должен использоваться механизм аутентификации на основе пароля.

5. Требования к созданию, присвоению и уничтожению идентификаторов

5.1. Создание, присвоение и уничтожение идентификатора должно осуществляться сотрудниками Института, назначенными ответственными за управление (администрирование) системой защиты информации и ответственными за обеспечение безопасности персональных данных (далее – Ответственный).

5.2. Ответственный обеспечивает однозначную идентификацию пользователя и (или) устройства путем формирования уникального персонального идентификатора.

5.3. Повторное использование идентификатора пользователя не допускается в течение одного года со дня уничтожения.

5.4. Блокирование идентификатора пользователя должно осуществляться после 30 дней неиспользования.

5.5. Идентификация устройств должна обеспечиваться одним или комбинацией следующих способов:

– по логическому имени (имя устройства и (или) ID);

– по логическому адресу (например, IP-адресу);

– по физическому адресу (например, MAC-адресам) устройства.

5.6. Уничтожение идентификатора пользователя производится при прекращении полномочий (увольнении) сотрудника.

6. Управление средствами аутентификации

6.1. Генерация (назначение) паролей

6.1.1. Генерация и выдача начальной аутентификационной информации (пароля) пользователю осуществляется Ответственным.

6.1.2. Средства, реализующие идентификацию и аутентификацию пользователей должны обеспечивать настройку характеристик паролей, представленных в таблице 2.

Таблица 2 – Требования к настройкам характеристик паролей

№ п/п	Характеристика	Значение	Примечание
1.	Минимальная длина пароля	8	Минимальное количество знаков, которое должно содержаться в пароле
2.	Соответствие требованиям к сложности пароля	Включено	Не содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков. Содержать знаки минимум трех из четырех перечисленных ниже категорий: - латинские заглавные буквы (от A до Z); - латинские строчные буквы (от a до z); - цифры (от 0 до 9) - специальные символы (например, !, $, #, %).
3.	Максимальный срок действия пароля	30 дней	Период времени (в днях), в течение которого можно использовать пароль, пока система не потребует от пользователя сменить его
4.	Максимальное количество неуспешных попыток аутентификации	5	Максимальное количество неуспешных попыток ввода неправильного пароля до блокировки
5.	Минимального количества измененных символов при создании новых паролей	5	Минимальное количество символов, которые требуется изменить при создании нового пароля по отношению к старому паролю
6.	Журнал паролей	4	При создании новых паролей запрещается использование пользователями определенного количества последних использованных паролей

6.2. Хранение паролей

6.2.1. Средства, реализующие идентификацию и аутентификацию, должны обеспечивать защиту аутентификационной информации от несанкционированного доступа к ней и ее модификации.

6.3. Порядок смены аутентификационной информации

6.3.1. Смена паролей производится на плановой и внеплановой основе.

6.3.2. Плановая смена паролей осуществляется при истечении максимального срока действия пароля.

6.3.3. Внеплановая смена паролей осуществляется в следующих случаях:

– компрометация или подозрение в компрометации пароля;

– прекращение полномочий (увольнение, изменение обязанностей и другие обстоятельства) сотрудников Института;

– по указанию сотрудника Института, назначенного ответственным за защиту информации;

– по указанию сотрудника Института, назначенного ответственным за обеспечение безопасности персональных данных.

6.4. Защита обратной связи при вводе пароля

6.4.1. Средства, реализующие идентификацию и аутентификацию, должны обеспечивать исключение отображения для пользователя действительного значения аутентификационной информации. Вводимые символы пароля должны отображаться условными знаками: «*», «●» или иными знаками.

7. Действия при компрометации аутентификационной информации

7.1. Компрометация действующих паролей является внештатной ситуацией.

7.2. Обо всех фактах компрометации паролей следует немедленно уведомить сотрудников Института, выполняющих функции по выявлению инцидентов информационной безопасности и реагированию на них.

7.3. Скомпрометированные пароли и связанные с ними персональные идентификаторы (логины) пользователей должны блокироваться при обнаружении факта компрометации.

8. Ответственность

8.1. Сотрудники Института, назначенные ответственными за защиту информации и ответственными за обеспечение безопасности персональных данных, и сотрудники Института, выполняющие функции по управлению (администрированию) системой защиты информации, по управлению конфигурацией информационной системы и ее системы защиты информации, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

Приложение № 2
к приказу ГАУ ДПО «Смоленский областной
институт развития образования»
от «21» 10 2024г. №201-од

Регламент управления доступом в информационных системах ГАУ ДПО «Смоленский областной институт развития образования»

1. Общие положения

1.1. Настоящий Регламент разработан с целью установления ГАУ ДПО «Смоленский областной институт развития образования» (далее – Институт) общих правил, требований и процедур управления доступом в информационных системах (далее – ИС) Института.

1.2. Меры защиты информации, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты информации, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты 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.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.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 субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники

1.3. Состав мер определен на основании установленного класса защищенности информационной системы, уровня защищенности персональных данных и структурно-функциональных характеристик ИС Института.

1.4. Правила и процедуры управления информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами описаны в рамках Регламента защиты информационной системы, ее средств, систем связи и передачи данных.

1.5. Регламент предназначен для сотрудников Института:

1.5.1. Назначенных ответственными за обеспечение безопасности персональных данных.

1.5.2. Назначенных ответственными за защиту информации.

1.5.3. Выполняющих функции по управлению (администрированию) системой защиты информации.

2. Термины и определения

2.1. Аутентификационная информация (информация аутентификации) – информация, используемая для установления подлинности (верификации) субъекта доступа в информационной (автоматизированной) системе.

2.2. Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной (автоматизированной) системе).

2.3. Идентификатор доступа (идентификатор) – уникальный признак субъекта или объекта доступа (представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной (автоматизированной) системе).

2.4. Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

2.5. Несанкционированный доступ – доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа.

2.6. Объект доступа – единица информационного ресурса информационной (автоматизированной) системы (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции.

2.7. Пароль – идентификатор субъекта доступа, который является его (субъекта) секретом.

2.8. Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной (автоматизированной) системе или использующее результаты ее функционирования.

2.9. Субъект доступа – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

2.10. Управление доступом – ограничение и контроль доступа субъектов доступа к объектам доступа в информационной (автоматизированной) системе в соответствии с установленными правилами разграничения доступа.

3. Требования к системе управления доступом

3.1. Управление доступом должно быть направлено на недопущение несанкционированного доступа к объектам доступа со стороны субъектов доступа, для которых запрашиваемый доступ не разрешен.

3.2. Доступ пользователей к информационным ресурсам ИС Института предоставляется сотрудниками Института, назначенными ответственными за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных), и сотрудниками Института, выполняющими функции по управлению (администрированию) системой защиты информации информационной системы (в отношении государственных информационных систем), исходя из следующих условий:

– доступ необходим для выполнения пользователем должностных обязанностей в соответствии со своей должностной инструкцией;

– доступ необходим для выполнения пользователем обязанностей другого пользователя по поручению (в виде служебной записки) руководителя соответствующего подразделения;

– доступ необходим для выполнения пользователем обязанностей другого пользователя по письменному указанию начальника Института;

– доступ необходим для выполнения пользователем работ по письменному указанию начальника Института;

– доступ необходим для выполнения пользователем работ в ходе реализации контрактов, договоров, заключенных с Институтом (для сотрудников «сторонних» организаций).

3.3. Физический доступ пользователей к техническим средствам ИС Института осуществляется в соответствии с установленным в Институте порядком доступа сотрудников Института в помещения, в которых осуществляется обработка информации и персональных данных.

3.4. Пользователи допускаются к информационному ресурсу на основании заявок, в соответствии с установленным порядком, представленным в пункте 7.

3.5. Допуск к информационному ресурсу предоставляется исключительно после ознакомления с локальными актами Института и прохождения обучения (инструктажа) по вопросам обеспечения информационной безопасности.

3.6. Средства вычислительной техники в информационных системах с 1 и 2 классом защищенности и информационных системах с уровнем защищенности персональных данных 1 и 2 должны быть оснащены средствами, исключающими несанкционированный доступ к программным и (или) техническим ресурсам средства вычислительной техники на этапе его загрузки. Функциональные возможности таких средств должны обеспечивать:

3.6.1. Блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы;

3.6.2. Контроль доступа пользователей к процессу загрузки операционной системы;

3.6.3. Контроль целостности программного обеспечения и аппаратных компонентов средства вычислительной техники на этапе его загрузки.

3.7. Доступ пользователей к программным функциям технических средств ИС Института должен осуществляться в соответствии с правилами разграничения доступа и с использованием учетных записей при успешном прохождении процедуры идентификации и аутентификации.

3.8. Средства, реализующие управление доступом, должны обеспечивать:

3.8.1. Ограничение неуспешных попыток входа (доступа) в количестве 10 раз за период времени в неограниченно, а также обеспечивать блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем установленного ограничения.

3.8.2. Блокирование сеанса доступа пользователя после 5 минут его бездействия (неактивности) или по запросу пользователя. Блокирование должно обеспечить временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к ИС Института (без выхода). Для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса. Блокирование сеанса доступа пользователя должно сохраняться до прохождения им повторной идентификации и аутентификации.

4. Методы управления доступом

4.1. В ИС Института должен быть реализован ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа.

4.2. Список ролей определяется в отношении каждой ИС Института ответственными за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных) и ответственными за защиту информации (в отношении государственных информационных систем) с учетом особенностей функционирования ИС и должностных обязанностей (функций) сотрудников Института при эксплуатации ИС и ее системы защиты информации.

4.3. При этом, в обязательном порядке должны быть выделены роли, осуществляющие функции по:

– управлению функциями безопасности и средствами защиты информации.

– управлению (администрированию) базами данных, прикладным программным обеспечением, телекоммуникационным оборудованием, рабочими станциями и серверами;

– обработке информации и персональных данных;

– обслуживанию помещений, в которых размещаются технические средства информационной системы – уборка, обслуживание и ремонт инженерных систем и т.п.;

– обслуживанию, ремонту, настройке и контролю работы обеспечивающих функционирование информационной системы – технических средств и систем.

4.4. Каждой роли должны быть определены минимально необходимые права и привилегии, необходимые для обеспечения функционирования информационной системы.

4.5. Каждому сотруднику при предоставлении доступа в информационную систему должна быть определена одна из определенных ролей.

4.6. Сведения о ролях и их полномочиях детализируется в рамках приказа о системе разграничения доступа.

4.7. Полномочия пользователей могут уточняться сотрудником Института, назначенным ответственным за управление (администрирование) системой защиты информации, по согласованию с сотрудником Института, назначенным ответственным за защиту информации (в отношении государственных информационных систем) и (или) за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных), исходя из должностных обязанностей (функций), возложенных на пользователя.

5. Идентификация объектов доступа

5.1. Сотрудники Института, назначенные ответственными за защиту информации и за обеспечение безопасности персональных данных, исходя из должностных обязанностей (функций), возложенных на пользователей, должны идентифицировать (определить) объекты доступа, в отношении которых реализуется управление доступом.

5.2. В качестве объектов доступа следует рассматривать:

5.2.1. Из числа технических средств:

– автоматизированные рабочие места пользователей;

– серверное оборудование;

– оборудование, обеспечивающее функционирование информационной системы (сервер синхронизации времени, оборудование локальной вычислительной сети, источники бесперебойного питания и т.п.).

5.2.2. Из числа объектов файловой системы:

– файлы и каталоги системного программного обеспечения;

– пользовательский каталог;

– запускаемые и исполняемые модули прикладного программного обеспечения;

– конфигурационные файлы прикладного программного обеспечения;

– запускаемые и исполняемые модули программного обеспечения средств защиты информации;

– конфигурационные файлы программного обеспечения средств защиты информации;

– файлы журналов регистрации событий безопасности;

– контейнеры (файлы), в которых хранится аутентификационная информация (или ее образы) пользователей.

5.3. Подробный состав объектов доступа в отношении каждой ИС Института детализируется в рамках приказа о системе разграничения доступа.

6. Типы доступа

6.1. В рамках управления доступа должны рассматриваться следующие типы доступа:

– физический доступ к техническим средствам;

– доступ к объектам файловой системы.

6.2. В качестве разрешенных к выполнению пользователю или запускаемому от его имени процессу при доступе к объектам файловой системы должны рассматриваться следующие операции:

– чтение (r);

– запись (w);

– удаление (d);

– выполнение (e).

7. Порядок предоставления доступа

7.1. Формирование запроса

7.1.1. Предоставление доступа к ИС Института осуществляется на основании заявок. Формирование заявки осуществляет либо сам сотрудник, которому необходимо предоставить доступ, либо руководитель сотрудника. Работа с заявками осуществляется в соответствии с установленным Институтом порядком. При этом, в заявке в обязательном порядке должен быть указан информационный ресурс, к которому необходим доступ, уровень доступа к нему, период, на который требуется предоставление доступа, и обоснование необходимости предоставления доступа.

7.1.2. Все заявки на предоставление доступа должны храниться сотрудниками Института, назначенными ответственными за защиту информации (в отношении государственных информационных систем) и за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных), и могут впоследствии использоваться для:

– контроля правомерности предоставления доступа при разборе инцидентов информационной безопасности и конфликтных ситуаций;

– проверки корректности предоставления доступа к информационным ресурсам.

7.2. Согласование предоставление доступа

7.2.1. Все сформированные заявки на доступ подлежат согласованию.

7.2.2. Согласование производится с:

– руководителем подразделения (если заявка сформирована сотрудником подразделения);

– сотрудником Института, назначенным ответственным за защиту информации (в отношении государственных информационных систем) и (или) за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных);

– лицами, согласование доступа с которыми предусмотрено в рамках внутренних локальных нормативных актов Института.

7.2.3. Сотрудник Института, назначенный ответственным за защиту информации и за обеспечение безопасности персональных данных, в процессе согласования должен выполнить:

– верификацию пользователя – проверку личности пользователя, его

должностных (функциональных) обязанностей;

– оценку обоснованности доступа к информационному ресурсу и запрашиваемого уровня доступа.

7.3. Ознакомление с документацией

7.3.1. Перед предоставлением доступа в обязательном порядке следует их ознакомить с локальными нормативными актами в области обеспечения безопасности информации и персональных данных.

7.3.2. Ознакомление должно производиться ответственным за защиту информации (в отношении государственных информационных систем) и за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных). Факты ознакомления должны фиксироваться в листах ознакомления и/или соответствующих журналах.

7.4. Предоставление доступа

7.4.1. Процесс предоставления доступа включает:

– создание сотрудником Института, назначенным ответственным за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных) или выполняющим функции по управлению (администрированию) системой защиты информации информационной системы (в отношении государственных информационных систем), учетной записи пользователя. Формирование реквизитов учетной записи (идентификатора и начальной аутентификационной информации (пароля)) осуществляется в соответствии с Регламентом идентификации и аутентификации;

– настройка средств защиты информации сотрудником Института, назначенным ответственным за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных) или выполняющим функции по управлению (администрированию) системой защиты информации информационной системы (в отношении государственных информационных систем);

– настройка программного обеспечения автоматизированного рабочего места и/или сервера сотрудником Института, назначенным ответственным за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных) или выполняющим функции по управлению (администрированию) системой защиты информации информационной системы (в отношении государственных информационных систем);

7.4.2. Предоставление доступа пользователю должно осуществляться в течение 2-х рабочих дней со дня согласования заявки.

7.5. Дополнительные сведения

7.5.1. Доступ пользователям к информационным ресурсам может быть предоставлен без оформления заявки в случае письменного указания руководства Института.

7.5.2. Доступ сотрудниками федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, иных государственных органов, органов прокуратуры и других правоохранительных органов, осуществляющих контрольные мероприятия и обладающих соответствующими полномочиями, осуществляется в соответствии с порядком, установленным законодательством Российской Федерации.

8. Порядок прекращения доступа

8.1. Доступ к ИС Института должен быть незамедлительно прекращен:

– при истечении срока предоставления доступа;

– при прекращении полномочий пользователя;

– по указанию руководства Института;

– по указанию сотрудника, назначенным ответственными за обеспечение безопасности персональных данных;

– по указанию сотрудника, назначенным ответственными за защиту информации;

– в случаях обнаружения факта компрометации учетной записи пользователя.

9. Ответственность

9.1. Сотрудники Института, назначенные ответственными за защиту информации и ответственными за обеспечение безопасности персональных данных, и сотрудники Института, выполняющие функции по управлению (администрированию) системой защиты информации, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

Приложение № 3
к приказу ГАУ ДПО «Смоленский областной
институт развития образования»
от «21» 10 2024 г. №201-од

Регламент ограничения программной среды в информационных системах ГАУ ДПО «Смоленский областной институт развития образования»

1. Общие положения

1.1. Настоящий Регламент разработан с целью установления ГАУ ДПО «Смоленский областной институт развития образования» (далее – Институт) общих правил, требований и процедур ограничения программной среды в информационных системах (далее – ИС) Института.

1.2. Меры защиты информации, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты информации, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты информации
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов

1.3. Состав мер определен на основании установленного класса защищенности информационной системы, уровня защищенности персональных данных и структурно-функциональных характеристик ИС Института.

1.4. Регламент предназначен для сотрудников Института:

1.4.1. Назначенных ответственными за обеспечение безопасности персональных данных.

1.4.2. Выполняющих функции по управлению конфигурацией информационной системы и ее системы защиты информации.

2. Управление установкой (инсталляцией) компонентов программного обеспечения

2.1. В ИС Института должна быть ограничена возможность установки программного обеспечения и его компонентов после загрузки операционной системы средства вычислительной техники.

2.2. Установка и настройка программного обеспечения и его компонентов должна быть доступна только сотрудникам Института, назначенным ответственными за обеспечение безопасности персональных данных и сотрудникам Института, выполняющим функции по управлению конфигурацией информационной системы и ее системы защиты информации.

2.3. Допускается установка только программного обеспечения и его компонентов, включенных в утвержденный начальником Института перечень программного обеспечения, разрешенного к использованию в ИС Института.

2.4. При установке программного обеспечения и его компонентов необходимо руководствоваться следующими правилами:

2.4.1. Исключить установку (если осуществимо) компонентов программного обеспечения, использование которых не требуется для реализации возложенных задач.

2.4.2. Отключение (если осуществимо) компонентов программного обеспечения, использование которых не требуется для реализации возложенных задач.

2.4.3. Применение параметров настройки компонентов программного обеспечения, включая программные компоненты средств защиты информации, обеспечивающих реализацию мер защиты информации, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации.

3. Ответственность

3.1. Сотрудники Института, выполняющие функции по управлению конфигурацией информационной системы и ее системы защиты информации, ответственные за обеспечение безопасности персональных данных, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

Приложение № 4
к приказу ГАУ ДПО «Смоленский областной
институт развития образования»
от «21» 10 2024 г. №201-од

Регламент защиты машинных носителей в информационных системах ГАУ ДПО «Смоленский областной институт развития образования»

1. Общие положения

1.1. Настоящий Регламент разработан с целью установления ГАУ ДПО «Смоленский областной институт развития образования» (далее – Институт) общих правил, требований и процедур ограничения защиты машинных носителей информации, используемых для хранения и обработки информации в информационных системах (далее – ИС) Института.

1.2. Меры защиты информации, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты информации, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты информации
ЗНИ.1	Учет машинных носителей информации
ЗНИ.2	Управление доступом к машинным носителям информации
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители 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)

1.3. Состав мер определен на основании установленного класса защищенности информационной системы, уровня защищенности персональных данных и структурно-функциональных характеристик ИС Института.

1.4. В качестве машинных носителей информации в настоящем Регламенте рассматриваются:

– машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках);

– съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства).

1.5. К использованию в информационных системах, являющихся государственными системами, и информационных системах, обрабатывающих персональные данные, допускаются только принятые к учету машинные носители информации.

1.6. Регламент предназначен для сотрудников Института:

1.6.1. Назначенных ответственными за обеспечение безопасности персональных данных.

1.6.2. Выполняющих функции по управлению конфигурацией информационной системы и ее системы защиты информации.

2. Термины и определения

2.1. Информация – сведения (сообщения, данные) независимо от формы их представления.

2.2. Идентификатор доступа (идентификатор) – уникальный признак субъекта или объекта доступа (представление (строка символов), однозначно идентифицирующий субъект и (или) объект доступа в информационной (автоматизированной) системе).

2.3. Несанкционированный доступ – доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа.

2.4. Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

2.5. Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной (автоматизированной) системе или использующее результаты ее функционирования.

3. Порядок учета машинных носителей информации

3.1. Положения данного раздела должны применяться только в отношении государственных информационных систем независимо от установленного класса защищенности и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1 или 2.

3.2. Учету подлежат все используемые в информационной системе машинные носители информации.

3.3. Учет машинных носителей информации должен осуществляться на основе регистрационных (учетных) номеров, нанесенных на носитель. В качестве регистрационных номеров могут использоваться:

– идентификационные (серийные) номера машинных носителей, присвоенные производителями этих машинных носителей информации;

– номера инвентарного учета.

3.4. Машинные носители информации, встроенные в корпуса средств вычислительной техники, подлежат учету в составе средств вычислительной техники. В таких случаях в качестве регистрационного номера машинного носителя может выступать регистрационный номер средства вычислительной техники.

3.5. Учет съемных машинных носителей информации должен осуществляться в журнале учета машинных носителей информации. Форма журнала учета машинных носителей информации утверждается начальником Института организационно-распорядительным документом.

3.6. Принятие на учет и ведение журнала учета осуществляется сотрудниками Института, назначенными ответственными за защиту информации и ответственными за обеспечение безопасности персональных данных.

3.7. При принятии на учет в обязательном порядке должна быть выполнена процедуру антивирусной проверки машинного носителя информации.

4. Порядок выдачи и возврата съемных машинных носителей информации

4.1. Положения данного раздела должны применяться только в отношении государственных информационных систем независимо от установленного класса защищенности и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1 или 2.

4.2. Учет выдачи и возврата съемных машинных носителей информации должен осуществляться сотрудником Института, назначенным ответственным за обеспечение безопасности персональных данных, и сотрудником Института, назначенным ответственным за защиту информации, с фиксацией действия в журнале учета машинных носителей информации.

4.3. При регистрации факта выдачи должны указываться:

– регистрационный номер носителя;

– дата и время выдачи;

– фамилия, имя и отчество должностного лица (работника), получившего носитель, и его подпись.

4.4. При возврате указывается дата и время.

4.5. Передача съемного машинного носителя информации между пользователями информационной системы не допускается.

4.6. При возврате носителя должна быть выполнена антивирусная проверка носителя.

4.7. В случае утраты пользователем съемного машинного носителя информации в журнале учета выдачи съемных машинных носителе информации заносится отметка об утрате.

5. Порядок доступа и хранения машинным носителям информации

5.1. Положения данного раздела должны применяться только в отношении государственных информационных систем независимо от установленного класса защищенности и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1 или 2.

5.2. Хранение машинных носителей информации должно осуществляться в местах, исключающих несанкционированный физический доступ.

5.3. Физический доступ к машинным носителям информации должны иметь только те лица, которым он необходим для выполнения своих должностных обязанностей (функций).

5.4. Перечень должностных лиц (сотрудников), имеющих право физического доступа к машинным носителям информации определяется внутренним организационно-распорядительным документом Института.

5.5. Доступ к машинным носителям информации, встроенным в корпус средств вычислительной техники (накопители на жестких дисках), должен осуществляться в соответствии с порядком доступа в помещения, в которых они размещены.

5.6. Ответственным за хранение машинных носителей информации, встроенных в корпус средства вычислительной техники, является пользователь средства вычислительной техники.

5.7. Ответственным за хранение съемных машинных носителей информации, является пользователь съемного машинного носителя информации.

6. Порядок списания машинных носителей информации и уничтожения (стирания) информации на них

6.1. Уничтожение информации с машинных носителей информации должно инициироваться пользователем и осуществляться средствами программного обеспечения. Параметры настроек программного обеспечения должны быть настроены таким образом, чтобы исключить возможность восстановления защищаемой информации.

6.2. В обязательном порядке уничтожение защищаемой информации с машинного носителя информации должно осуществляться при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации.

6.3. Машинные носители информации, пришедшие в негодность или отслужившие установленный срок подлежат списанию или уничтожению.

6.4. Уничтожение персональных данных с машинных носителей информации должно выполняться комиссией по уничтожению персональных данных в соответствии с Правилами по уничтожению персональных данных в ГАУ ДПО «Смоленский областной институт развития образования», утвержденными локальным актом Института.

7. Использование интерфейсов ввода (вывода) информации

7.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности 1 или 2.

7.2. Разрешенными интерфейсами средств вычислительной техники, которые могут использоваться для ввода (вывода) информации, являются:

– интерфейсы устройств для ввода (вывода) информации (клавиатура, мышь, монитор, принтер и т.д.);

– интерфейсы сетевого взаимодействия.

7.3. К интерфейсам, не включенным в список разрешенных к использованию, должны быть приняты меры, исключающие возможность их использования. В качестве таких мер могут выступать:

– опечатывание интерфейсов ввода (вывода);

– использование механических запирающих устройств;

– удаление драйверов, обеспечивающих работу интерфейсов ввода (вывода);

– применение средств защиты информации, обеспечивающих контроль использования интерфейсов ввода (вывода).

7.4. Программное обеспечение средств вычислительной техники должно обеспечивать регистрацию действий пользователей по подключению машинного носителя информации. Состав регистрируемых событий определяется регламентом аудита безопасности.

7.5. Сотрудники Института, назначенные ответственными за защиту информации и ответственными за обеспечение безопасности персональных данных, должны периодически в информационных системах, являющихся государственными системами с установленным классом защищенности 1 и 2, организовывать проведение мероприятий по контролю использования интерфейсов ввода (вывода) информации. Мероприятия по контролю использования интерфейсов ввода (вывода)

информации должны быть включены в ежегодный план мероприятий по защите информации.

8. Ответственность

8.1. Сотрудники Института, назначенные ответственными за защиту информации и ответственными за обеспечение безопасности персональных данных, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

Приложение № 5
к приказу ГАУ ДПО «Смоленский областной
институт развития образования»
от «21» 10 2024 г. №201-од

Регламент регистрации событий безопасности в информационных системах ГАУ ДПО «Смоленский областной институт развития образования»

1. Общие положения

1.1. Настоящий Регламент разработан с целью установления ГАУ ДПО «Смоленский областной институт развития образования» (далее – Институт) общих правил, требований и процедур регистрации событий безопасности в информационных системах (далее – ИС) Института.

1.2. Меры защиты информации, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты информации, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты 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 течение установленного времени хранения
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе
РСБ.7	Защита информации о событиях безопасности

1.3. Состав мер определен на основании установленного класса защищенности информационной системы, уровня защищенности персональных данных и структурно-функциональных характеристик ИС Института.

1.4. Положения раздела 2.3 настоящего регламента должны применяться только в отношении государственных информационных систем независимо от установленного класса защищенности и информационных систем персональных данных с установленным уровнем защищенности персональных данных 1 или 2.

1.5. Положения раздела 2.4 настоящего регламента должны применяться только в отношении государственных информационных систем независимо от установленного класса защищенности.

1.6. Регламент предназначен для сотрудников Института:

1.6.1. Назначенных ответственными за обеспечение безопасности персональных данных.

1.6.2. Назначенных ответственными за защиту информации.

1.6.3. Выполняющих функции по управлению (администрированию) системой защиты информации.

1.6.4. Выполняющих функции по управлению конфигурацией информационной системы и ее системы защиты информации.

2. Регистрация и мониторинг событий безопасности

2.1. Общие положения

2.1.1. Сбор, запись и хранение информации о событиях безопасности осуществляется с целью выявления инцидентов информационной безопасности и реагирования на них.

2.1.2. Сбор, запись и хранение событий безопасности должны осуществляться на всех компонентах ИС (рабочие места пользователей, серверы, телекоммуникационное оборудование). Требования к составу и содержанию информации о событиях безопасности представлены в пункте 2.2.

2.1.3. Все компоненты ИС, осуществляющие регистрацию событий безопасности, должны синхронизироваться с единым источником точного времени.

2.1.4. Доступ к функциям управления механизмами регистрации (аудита) должен быть доступен только сотрудникам Института, выполняющим функции по управлению конфигурацией информационной системы и ее системы защиты информации.

2.1.5. Доступ к записям аудита должен быть доступен только сотрудникам Института:

– Назначенным ответственными за обеспечение безопасности персональных данных.

– Выполняющим функции по управлению (администрированию) системой защиты информации.

– Выполняющим функции по управлению конфигурацией информационной системы и ее системы защиты информации.

– Выполняющим функции по выявлению инцидентов информационной безопасности и реагирование на них.

2.1.6. Защита информации о событиях безопасности (записях регистрации (аудита)) должна обеспечиваться применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования. В том числе должна обеспечиваться защита средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

2.1.7. Зарегистрированные события безопасности должны храниться не менее 3-х лет.

2.2. Требования к составу регистрируемых событий безопасности

2.2.1. Регистрации подлежать следующие события, представленные в таблице 2.

Таблица 2 – Состав и содержание информации о событиях безопасности

№ п/п	Событие	Минимальный состав информации о событии
1.	Вход (выход), а также попытки входа субъектов доступа (пользователей) в операционную систему	Дата и время входа (выхода) в операционную систему (из операционной системы); Результат попытки входа (успешный или неуспешный); Идентификатор (логин), предъявленный при попытке доступа
2.	Изменение полномочий субъектов доступа и статуса объектов доступа, в том числе создание, модификация, удаление учетных записей	Дата и время создания или модификации или удаления учетной записи или статуса объекта доступа; Результат операции (успешный или неуспешный); Идентификатор (логин) субъекта доступа (пользователя), выполнившего операцию (создание или модификация или удаление учетной записи / изменении статуса объекта доступа)
3.	Подключение съемных машинных носителей информации и вывод информации на носители информации	Дата и время подключения съемного машинного носителя информации и вывода информации на носители информации; Логическое имя (имя устройства и (или) ID) съемного машинного носителя информации; Идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации
4.	Запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации	Дата и время запуска; Имя (идентификатор) программы (процесса, задания); Идентификатор субъекта доступа (пользователя, устройства), запросившего программу (процесс, задание); Результат запуска (успешный, неуспешный)
5.	Попытки доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам	Дата и время попытки доступа к защищаемому файлу; Результат попытки доступа (успешный, неуспешный); Идентификатор субъекта доступа (пользователя, устройства); Спецификация защищаемого файла (логическое имя, тип)
6.	Попытки доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей)	Дата и время попытки доступа к защищаемому объекту; Результата попытки доступа (успешный, неуспешный); Идентификатор субъекта доступа (пользователя, устройства); Спецификацию защищаемого объекта доступа (логическое имя (номер))

2.3. Мониторинг событий безопасности

2.3.1. Мониторинг событий безопасности осуществляется сотрудниками Института, назначенными ответственными за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных), и сотрудниками Института, выполняющими функции по управлению (администрированию) системой защиты информации информационной системы (в отношении государственных информационных систем).

2.3.2. Мониторинг подразумевает периодический просмотр и анализ записей регистрации (аудита).

2.3.3. В случае выявления признаков инцидентов информационной безопасности должно осуществляться информирование сотрудников Института, выполняющих функции по выявлению инцидентов информационной безопасности и реагирование на них. Реагирование на инциденты информационной безопасности должно осуществляться в соответствии с установленным в инструкции порядком.

2.4. Реагирование на сбои при регистрации событий безопасности

2.4.1. В качестве сбоя при регистрации событий безопасности должны рассматриваться:

– сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки;

– сбои в механизмах сбора информации;

– переполнения объема (емкости) памяти при регистрации событий безопасности.

2.4.2. Для своевременного выявления всех случаев сбоя настройки средств, осуществляющих регистрацию событий безопасности, должно обеспечиваться незамедлительное (в масштабе времени, близком к реальному) предупреждение (индикация, сигнализация) сотрудников Института, выполняющих функции по управлению конфигурацией информационной системы и ее системы защиты информации.

2.4.3. Реагирование на сбои при регистрации событий безопасности должно осуществляться сотрудником Института, выполняющим функции по управлению конфигурацией информационной системы и ее системы защиты информации. Реагирование осуществляется путем изменения параметров сбора, записи и хранения информации о событиях безопасности (отключение записи информации о событиях безопасности от части компонентов информационной системы; запись поверх устаревших хранимых записей событий безопасности и т.д.) с фиксацией факта выполненного действия в журнале учета нештатных ситуаций.

3. Ответственность

3.1. Сотрудники Института, назначенные ответственными за защиту информации и ответственными за обеспечение безопасности персональных данных, и сотрудники Института, выполняющие функции по управлению (администрированию) системой защиты информации, по управлению конфигурацией информационной системы и ее системы защиты информации, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

Приложение № 6
к приказу ГАУ ДПО «Смоленский областной
институт развития образования»
от «21» 10 2024 г. №201-ф

Регламент антивирусной защиты в информационных системах ГАУ ДПО «Смоленский областной институт развития образования»

1. Общие положения

1.1. Настоящий Регламент разработан с целью установления ГАУ ДПО «Смоленский областной институт развития образования» (далее – Институт) порядка организации защиты от угроз, связанных с внедрением вредоносных компьютерных программ (вирусов) из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования), и съемных машинных носителей информации в информационных системах (далее – ИС) Института.

1.2. Меры защиты информации, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты информации, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты информации
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

1.3. Состав мер определен на основании установленного класса защищенности информационной системы, уровня защищенности персональных данных и структурно-функциональных характеристик ИС Института.

1.4. Регламент предназначен для сотрудников Института:

1.4.1. Назначенных ответственными за обеспечение безопасности персональных данных.

1.4.2. Назначенных ответственными за защиту информации.

1.4.3. Выполняющих функции по управлению (администрированию) системой защиты информации.

1.4.4. Выполняющих функции по планированию мероприятий по защите информации.

1.4.5. Выполняющих функции по управлению конфигурацией информационной системы и ее системы защиты информации.

2. Термины и определения

2.1. Антивирусная защита – защита информации и компонентов информационной системы от вредоносных компьютерных программ (вирусов) (обнаружение вредоносных компьютерных программ (вирусов), блокирование, изолирование «зараженных» объектов, удаление вредоносных компьютерных программ (вирусов) из «зараженных» объектов).

2.2. Безопасность информации – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

2.3. Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы.

2.4. Компьютерный вирус – программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

2.5. Сигнатура – характерные признаки компьютерной вредоносной программы (вируса), используемые для ее обнаружения.

2.6. Угроза безопасности информации – совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения безопасности информации.

2.7. Управление доступом – ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа.

3. Требования к антивирусной защите

3.1. Для реализации антивирусной защиты на всех компонентах ИС Института должны применяться средства антивирусной защиты.

3.2. Антивирусная защита должна быть реализована:

– на автоматизированных рабочих местах пользователей (в том числе привилегированных пользователей);

– в среде виртуализации;

– на серверах.

3.3. Установка (инсталляция), настройка (конфигурирование), обновление модулей средств антивирусной защиты, удаление должны осуществляться только сотрудниками Института, назначенными ответственными за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных) и сотрудниками Института, выполняющими функции по управлению (администрированию) системой защиты информации информационной системы (в отношении государственных информационных систем).

3.4. Управление параметрами настройки функций безопасности средств антивирусной защиты должно быть доступно только сотрудникам Института, назначенным ответственными за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных) и сотрудникам Института, выполняющим функции по управлению (администрированию) системой защиты информации информационной системы (в отношении государственных информационных систем).

3.5. Средства антивирусной защиты должны постоянно находиться в активном состоянии и обеспечивать антивирусную защиты в режиме реального времени.

3.6. Автоматическое обновление модулей средств антивирусной защиты должно быть запрещено.

3.7. Обновление модулей средств антивирусной защиты должно производиться сотрудниками Института, назначенными ответственными за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных), и сотрудниками Института, выполняющими функции по управлению (администрированию) системой защиты информации информационной системы (в отношении государственных информационных систем), в «ручном» режиме и только по согласованию с сотрудником Института, выполняющим функции по управлению конфигурацией информационной системы и ее системы защиты информации.

4. Требования к параметрам настроек средств антивирусной защиты

4.1. Периодичность поиска вредоносных компьютерных программ (вирусов) средствами антивирусной защиты должно обеспечиваться в соответствии с таблицей 2.

Таблица 2 – Периодичность поиска вирусов

№ п/п	Объект проверки	Частота проверки
1.	Системная память	Не реже одного раза в сутки
2.	Объекты (файлы), загружаемые при старте операционной системы	Не реже одного раза в сутки
3.	Объекты (файлы), поступающие по каналам передачи данных	Каждый раз перед открытием (запуском) объекта (файла)
4.	Файлы инсталляции программного обеспечения	Каждый раз перед установкой (инсталляцией)
5.	Файлы обновлений программного обеспечения	Каждый раз перед обновлением программного обеспечения
6.	Машинные носители информации, встроенных в портативные или стационарные технические средства	Не реже одного раза в неделю
7.	Съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные носители)	Каждый раз при подключении

4.2. Антивирусная проверка должна осуществляться современными методами обнаружения вредоносных компьютерных программ (вирусов), в том числе включать:

– сигнатурный метод. Метод, основанный на поиске в объектах (файлах) сигнатур известных компьютерных вирусов;

– метод обнаружения изменений. Метод, основанный на предварительном запоминании характеристик всех областей диска, которые могут подвергаться нападению компьютерными вирусами, и их периодической проверке на изменения;

– методы резидентных сторожей. Метод, основанный на отслеживании всех подозрительных действий, выполняемых другими программами;

– методы эвристического анализа (эвристического сканирования).

4.3. Средства антивирусной защиты при обнаружении вредоносной компьютерной программы (вируса) должны выполнять следующие действия:

– зафиксировать в журнале регистрации событий факт обнаружения вредоносной компьютерной программы (вируса);

– удалить зараженный объект (файла) либо переместить его в карантин;

– уведомить в масштабе времени, близком к реальному, об обнаружении

вредоносной компьютерной программы (вируса).

4.4. Средства антивирусной защиты должны обеспечивать регистрацию событий, связанных с функционированием, включая:

– проведение проверок объектов на наличие вредоносных компьютерных программ (вирусов);

– отказ работоспособности средства антивирусной защиты и его компонентов;

– обнаружение вредоносной компьютерной программы (вируса);

– изменение конфигурации средства антивирусной защиты;

– обновление модулей средства антивирусной защиты и базы данных признаков вредоносных компьютерных программ (вирусов).

4.5. Журналы регистрации событий средств антивирусной защиты должны храниться не менее 1 года и должны быть доступны для оперативного анализа в течение 1 месяца после регистрации событий.

5. Требования к обновлению базы данных признаков вредоносных компьютерных программ (вирусов)

5.1. Сотрудники Института, назначенные ответственными за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных), и сотрудники Института, выполняющие функции по управлению (администрированию) системой защиты информации информационной системы (в отношении государственных информационных систем), должны обеспечить обновление базы данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты по факту их выпуска производителем средства антивирусной защиты.

5.2. Базы данных признаков вредоносных компьютерных программ (вирусов) должны быть получены из доверенных источников. В качестве доверенных источников следует рассматривать официальные сайты производителей используемых средств защиты информации.

5.3. Сотрудники Института, назначенные ответственными за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных), и сотрудники Института, выполняющие функции по управлению (администрированию) системой защиты информации информационной системы (в отношении государственных информационных систем), должны периодически проводить мероприятие по контролю обновления баз данных признаков вредоносных компьютерных программ (вирусов). Мероприятие должно быть включено в ежегодный план мероприятий по защите информации.

6. Действия при обнаружении вредоносных компьютерных программ (вирусов)

6.1. При обнаружении вредоносных компьютерных программ (вирусов) сотрудники Института, назначенные ответственными за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных), и сотрудники Института, выполняющие функции по управлению (администрированию) системой защиты информации информационной системы (в отношении государственных информационных систем), должны сообщить об этом сотруднику Института, выполняющему функции по выявлению инцидентов информационной безопасности и реагированию на них. Данные лица совместно

принимают меры по предотвращению наступления негативных последствий заражения. Меры могут включать:

– остановку эксплуатации зараженного компонента информационной системы и (или) изоляцию его от остальных компонентов;

– удаление вредоносной программы;

– установление причин и источника заражения;

– инициацию и проведение служебной проверки по факту заражения вредоносной компьютерной программой (вирусом). Принятие мер по минимизации возможности подобных заражений в дальнейшем;

– проведение полной антивирусной проверки всех компонентов информационной системы.

6.2. Возобновление работы с компонентом информационной системы, подвергшимся заражению, осуществляется только после окончания работ по удалению вредоносных программ и проведения антивирусной проверки прочих объектов (файлов).

7. Ответственность

7.1. Сотрудники Института, назначенные ответственными за защиту информации и ответственными за обеспечение безопасности персональных данных, и сотрудники Института, выполняющие функции по управлению (администрированию) системой защиты информации, по планированию мероприятий по защите информации, по управлению конфигурацией информационной системы и ее системы защиты информации, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

Приложение № 7
к приказу ГАУ ДПО «Смоленский областной
институт развития образования»
от «21» 10 2024 г. № 201-од

Регламент обнаружения вторжений в информационных системах ГАУ ДПО «Смоленский областной институт развития образования»

1. Общие положения

1.1. Настоящий Регламент разработан с целью установления ГАУ ДПО «Смоленский областной институт развития образования» (далее – Институт) общих правил, требований и процедур защиты от компьютерных атак в информационных системах (далее – ИС) Института.

1.2. Меры защиты информации, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты информации, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты информации
СОВ.1	Обнаружение вторжений
СОВ.2	Обновление базы решающих правил

1.3. Состав мер определен на основании установленного класса защищенности информационной системы, уровня защищенности персональных данных и структурно-функциональных характеристик ИС Института.

1.4. Регламент предназначен для сотрудников Института:

1.4.1. Назначенных ответственными за обеспечение безопасности персональных данных.

1.4.2. Назначенных ответственными за защиту информации.

1.4.3. Выполняющих функции по управлению (администрированию) системой защиты информации.

1.4.4. Выполняющих функции по управлению конфигурацией информационной системы и ее системы защиты информации.

2. Требования к обнаружению вторжений

2.1. Для обнаружения вторжений (компьютерных атак) должны применяться программные или программно-аппаратные средства, реализующие функции обнаружения вторжений.

2.2. В зависимости от особенностей функционирования ИС Института системы обнаружения вторжений (компьютерных атак) должны использоваться на внешних границах сети Института или ИС, или на узлах ИС: автоматизированных рабочих местах, серверах.

2.3. Принципы использования систем обнаружения (компьютерных атак) должны определяться в проектной документации на систему защиты информации с учетом функциональных и технологических особенностей процесса обработки информации и анализа угроз безопасности информации.

2.4. Применяемые системы обнаружения вторжений должны обеспечивать:
– регистрацию событий безопасности;
– анализ событий безопасности и распознавание компьютерных атак;
– использование базы решающих правил, содержащей информацию о характерных признаках компьютерных атак.

2.5. Управление параметрами настроек функций безопасности систем обнаружения вторжений должно быть доступно только сотрудникам Института, назначенным ответственными за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных), и сотрудникам Института, выполняющим функции по управлению (администрированию) системой защиты информации информационной системы (в отношении государственных информационных систем).

2.6. Системы обнаружения и предотвращения вторжений должны постоянно находиться в активном состоянии и обеспечивать защиту в масштабе времени, близком к реальному.

2.7. Обновление модулей средств обнаружения вторжений должно производиться сотрудниками Института, назначенными ответственными за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных), и сотрудниками Института, выполняющими функции по управлению (администрированию) системой защиты информации информационной системы (в отношении государственных информационных систем), в «ручном» режиме и только по согласованию с сотрудником Института, выполняющим функции по управлению конфигурацией информационной системы и ее системы защиты информации.

3. Требования к обновлению базы решающих правил

3.1. Для обнаружения вторжений (компьютерных атак) должны применяться программные или программно-аппаратные средств, реализующие функции обнаружения вторжений.

3.2. Сотрудники Института, назначенные ответственными за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных), и сотрудники Института, выполняющие функции по управлению (администрированию) системой защиты информации информационной системы (в отношении государственных информационных систем), должны обеспечить обновление базы решающих правил по факту их выпуска производителем средства обнаружения вторжений.

3.3. Базы решающих правил должны быть получены из доверенных источников. В качестве доверенных источников следует рассматривать официальные сайты производителей используемых средств обнаружения вторжений.

3.4. Сотрудники Института, назначенные ответственными за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных), и сотрудники Института, выполняющие функции по управлению (администрированию) системой защиты информации информационной системы (в отношении государственных информационных систем), должны периодически проводить мероприятие по контролю обновления баз решающих

правил. Мероприятие должно быть включено в ежегодный план мероприятий по защите информации.

4. Действия при обнаружении признаков вторжений (компьютерных атак)

4.1. При обнаружении признаков вторжений (компьютерных атак) системы обнаружения и предотвращения вторжений должны осуществлять:

– реагирование на компьютерные атаки в соответствии с правилами, определенными для информационной системы с учетом особенностей ее функционирования;

– уведомление сотрудников Института, осуществляющих функции по выявлению компьютерных инцидентов и реагированию на них.

5. Ответственность

5.1. Сотрудники Института, назначенные ответственными за защиту информации и ответственными за обеспечение безопасности персональных данных, и сотрудники Института, выполняющие функции по управлению (администрированию) системой защиты информации, по планированию мероприятий по защите информации, по управлению конфигурацией информационной системы и ее системы защиты информации, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

Приложение № 8
к приказу ГАУ ДПО «Смоленский областной
институт развития образования»
от «21» 10 2024г. №201-од

Регламент контроля (анализа) защищенности в информационных системах ГАУ ДПО «Смоленский областной институт развития образования»

1. Общие положения

1.1. Настоящий Регламент разработан с целью установления ГАУ ДПО «Смоленский областной институт развития образования» (далее – Институт) общих правил, требований и процедур контроля (анализа) защищенности в информационных системах (далее – ИС) Института.

1.2. Меры защиты информации, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты информации, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты информации
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 доступом, полномочий пользователей в информационной системе

1.3. Состав мер определен на основании установленного класса защищенности информационной системы, уровня защищенности персональных данных и структурно-функциональных характеристик ИС Института.

1.4. Регламент предназначен для сотрудников Института:

1.4.1. Назначенных ответственными за обеспечение безопасности персональных данных.

1.4.2. Назначенных ответственными за защиту информации.

2. Контроль установки обновлений программного обеспечения

2.1. Мероприятия по контролю установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации, должны проводиться на периодической основе и должны быть включены в ежегодный план мероприятий по защите информации. В ходе проведения данного мероприятия должно осуществляться:

2.1.1. Проверка использования последних версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации (проверка

соответствия версий – используемой и представленной на официальном сайте (портале) производителя (разработчика));

2.1.2. Проверка наличия отметок об установке (применении) обновлений в эксплуатационной документации (техническом паспорте).

2.1.3. Документирование результатов контроля.

2.1.4. При обнаружении фактов пропуска обновлений – уведомление сотрудника Института, выполняющего функции по управлению (администрированию) системой защиты информации.

3. Анализ уязвимостей и их устранение

3.1. Общие положения

3.1.1. Анализ уязвимостей направлен на снижение вероятности реализации нарушителем угроз, связанных с использованием (эксплуатацией) уязвимостей, опубликованных в общедоступных источниках (как минимум, опубликованных в банке данных угроз безопасности информации ФСТЭК России).

3.1.2. Мероприятия анализа уязвимостей должны проводиться на периодической основе (не реже раз в месяц) и должны быть включены в ежегодный план мероприятий по защите информации. Внеплановый поиск уязвимостей может быть произведен при появлении в общедоступных источниках информации (сведений) о новых уязвимостях, которые потенциально могут быть в информационной системе.

3.1.3. Анализ уязвимостей должен включать:

– выявление (поиск) уязвимостей, связанных с ошибками кода в программном обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации;

– проверку правильности установки и настройки средств защиты информации, технических средств и программного обеспечения;

– проверку корректности работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением.

3.1.4. Выявление (поиск) уязвимостей организуется сотрудниками Института, назначенными ответственными за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных) и ответственными за защиту информации (в отношении государственных информационных систем). Выявление (поиск) уязвимостей может производится как вручную, так и с использованием специализированных средств анализа защищенности (поиска уязвимостей). Для проведения выявления (поиска) уязвимостей могут привлекаться организации, имеющие лицензии на деятельность по технической защите конфиденциальной информации.

3.1.5. При использовании специализированных средств анализа защищенности (поиска уязвимостей) должно обеспечиваться периодическое обновление базы признаков уязвимостей таких средств.

3.1.6. Анализ уязвимостей должен быть осуществлен в отношении всех компонентов информационной системы: автоматизированные рабочие места пользователей, серверы, среда виртуализации (при наличии), телекоммуникационное оборудование и т.д.

3.2. Порядок анализа уязвимостей

3.2.1. Анализ уязвимостей должен быть проведен в следующем порядке:

– определение компонентов информационной системы, в отношении которых требуется проведение поиска уязвимостей;

– выявление (поиск) уязвимостей с использованием специализированных средств анализа защищенности (поиска уязвимостей) или вручную;

– оформление результатов поиска уязвимостей в виде отчета с описанием выявленных уязвимостей;

– анализ достаточности реализованных мер защиты информации.

– планирование мероприятий по устранению выявленных уязвимостей.

3.3. Порядок устранения уязвимостей

3.3.1. Устранение выявленных уязвимостей организуется сотрудниками Института, назначенными ответственными за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных), и ответственными за защиту информации (в отношении государственных информационных систем), и должно быть выполнено в соответствии с планом, сформированным по результатам анализа уязвимостей.

3.3.2. Устранение осуществляется в том числе путем:

– установки обновлений средств защиты информации, программного обеспечения, микропрограммного обеспечение технических средств.

– реализации действий, направленных на устранение возможности использования выявленных уязвимостей (настройки средств защиты информации, изменение режима и порядка использования значимого объекта).

3.3.3. Факты устранения уязвимостей должны отражаться в соответствующей эксплуатационной документации на информационную систему: журналах, формулярах, паспортах на технические средства и т.д.

4. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

4.1. Мероприятия по контролю работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации должны проводиться на периодической основе и должны быть включены в ежегодный план мероприятий по защите информации. В ходе проведения данного мероприятия должно осуществляться:

4.1.1. Проверка работоспособности (неотключения) программного обеспечения и средств защиты информации.

4.1.2. Проверка правильности функционирования программного обеспечения и средств защиты информации.

4.1.3. Проверка настроек программного обеспечения и средств защиты информации на соответствие настройкам, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации.

4.1.4. Восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

5. Контроль состава технических средств, программного обеспечения и средств защиты информации

5.1. Мероприятия по контролю состава технических средств, программного обеспечения и средств защиты информации должны проводиться на периодической основе и должны быть включены в ежегодный план мероприятий по защите информации. В ходе проведения данного мероприятия должно осуществляться:

5.1.1. Проверка состава технических средств, программного обеспечения и средств защиты информации информационной системы на соответствие сведениям о составе, приведенным в действующей эксплуатационной документации.

5.1.2. Проверка выполнения условий и сроков действия сертификатов соответствия на средства защиты информации.

5.1.3. Принятие мер, направленных на устранение выявленных недостатков. Исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

6. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе

6.1. Мероприятия по контролю состава технических средств, программного обеспечения и средств защиты информации должны проводиться на периодической основе и должны быть включены в ежегодный план мероприятий по защите информации. В ходе проведения данного мероприятия должно осуществляться:

6.1.1. Проверка соблюдения правил генерации и смены паролей пользователями.

6.1.2. Проверка соблюдения правил заведения и удаления учетных записей пользователей, предусмотренных регламентом управления доступом.

6.1.3. Проверка реализации правил разграничения доступом в соответствии с регламентом управления доступом и организационно-распорядительным документом об утверждении системы разграничения доступом в информационной системе.

6.1.4. Принятие мер, направленных на устранение выявленных недостатков.

7. Ответственность

7.1. Сотрудники Института, назначенные ответственными за защиту информации и ответственными за обеспечение безопасности персональных данных, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

Приложение № 9
к приказу ГАУ ДПО «Смоленский областной
институт развития образования»
от «21» 10 2024г. №201-од

Регламент обеспечения целостности в информационных системах ГАУ ДПО «Смоленский областной институт развития образования»

1. Общие положения

1.1. Настоящий Регламент разработан с целью установления ГАУ ДПО «Смоленский областной институт развития образования» (далее – Институт) общих правил, требований и процедур обеспечения целостности информационных систем (далее – ИС) Института и информации, в том числе персональных данных.

1.2. Меры защиты информации, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты информации, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты информации
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)

1.3. Состав мер определен на основании установленного класса защищенности информационной системы, уровня защищенности персональных данных и структурно-функциональных характеристик ИС Института.

1.4. Регламент предназначен для сотрудников Института:

1.4.1. Назначенных ответственными за защиту информации.

1.4.2. Выполняющих функции по управлению (администрированию) системой защиты информации.

1.4.3. Выполняющих функции по планированию мероприятий по защите информации.

1.4.4. Выполняющих функции по управлению конфигурацией информационной системы и ее системы защиты информации.

2. Контроль целостности программного обеспечения

2.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности 1 или 2 и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1 или 2.

2.2. Мероприятия по контролю целостности программного обеспечения должны проводиться на периодической основе и должны быть включены в ежегодный план мероприятий по защите информации.

2.3. Контроль целостности должен осуществляться в отношении:

– программного обеспечения средств защиты информации;

– системного программного обеспечения технических средств;

– общесистемного и прикладного программного обеспечения.

2.4. Контроль целостности программного обеспечения осуществляется путем проверки:

– его наличия в информационной системе по имени (идентификатору);

– контрольных сумм (в процессе его загрузки; и (или) динамически в процессе работы).

2.5. Проверка контрольных сумм программного обеспечения представляет из себя проверку соответствия значений контрольных сумм программного обеспечения, представленных в формулярах или зафиксированных в рабочей документации на информационную систему, значениям контрольных сумм, вычисленных во время мероприятия (проверки).

2.6. Результаты выполнения мероприятий по контролю целостности программного обеспечения должны оформляться актом по результатам контроля целостности.

2.7. В случае обнаружения фактов нарушения целостности программного обеспечения необходимо:

– зафиксировать факт нарушения целостности в акте по результатам контроля целостности;

– незамедлительно уведомить сотрудников Института, выполняющих функции по выявлению инцидентов информационной безопасности и реагированию на них;

– организовать расследование факта нарушения целостности;

– восстановить целостность в соответствии с порядком, предусмотренным, регламентом обеспечения доступности.

3. Обеспечение возможности восстановления программного обеспечения

3.1. Для обеспечения возможности восстановления программного обеспечения в информационной системе при возникновении нештатных ситуаций должны быть приняты соответствующие планы по действиям сотрудников Института.

3.2. Восстановление программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций должно предусматривать:

– восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий или дистрибутивов программного обеспечения;

– восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации;

– возврат информационной системы в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей информационной

системы, позволяющих решать задачи по обработке информации.

3.3. Восстановление программного обеспечения должно осуществляться сотрудниками Института, выполняющими функции по управлению (администрированию) системой защиты информации, по согласованию с сотрудниками Института, выполняющими функции по управлению конфигурацией информационной системы и ее системы защиты информации.

4. Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)

4.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности 1 или 2 и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1 или 2.

4.2. В информационных системах должно обеспечиваться обнаружение и реагирование на поступление незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной (автоматизированной) системы (защита от спама).

4.3. Защита от спама должна быть реализована на точках входа и выхода информационных потоков, а также на автоматизированных рабочих местах, серверах и мобильных технических средствах, подключенных к сетям связи общего пользования.

4.4. Защита от спама должна обеспечиваться применением программных и (или) программно-аппаратных средств, реализующих следующие механизмы защиты:

– фильтрация по содержимому электронных сообщений (писем, документов) с использованием критериев, позволяющих относить сообщения к спаму сигнатурным и (или) эвристическим методами;

– фильтрация на основе информации об отправителе электронного сообщения (в том числе с использованием «черных» списков (запрещенные отправители) и (или) «белых» списков (разрешенные отправители).

4.5. Сотрудники Института, выполняющие функции по управлению (администрированию) системой защиты информации, должны осуществлять периодическое обновление базы «черных» («белых») списков и контроль целостности базы «черных» («белых») списков.

5. Ответственность

5.1. Сотрудники Института, назначенные ответственными за защиту информации и ответственными за обеспечение безопасности персональных данных, и сотрудники Института, выполняющие функции по управлению (администрированию) системой защиты информации, по управлению конфигурацией информационной системы и ее системы защиты информации, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

Приложение № 10
к приказу ГАУ ДПО «Смоленский областной
институт развития образования»
от «21» 10 2024 г. №201-од

Регламент обеспечения доступности в информационных системах ГАУ ДПО «Смоленский областной институт развития образования»

1. Общие положения

1.1. Настоящий Регламент разработан с целью установления ГАУ ДПО «Смоленский областной институт развития образования» (далее – Институт) общих правил, требований и процедур обеспечения доступности информационных систем (далее – ИС) Института и информации, в том числе персональных данных.

1.2. Меры защиты информации, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты информации, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты информации
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала
ОДТ.7	Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации

1.3. Состав мер определен на основании установленного класса защищенности информационной системы, уровня защищенности персональных данных и структурно-функциональных характеристик ИС Института.

1.4. Регламент предназначен для сотрудников Института:

1.4.1. Назначенных ответственными за обеспечение безопасности персональных данных.

1.4.2. Назначенных ответственными за защиту информации.

1.4.3. Выполняющих функции по управлению (администрированию) системой защиты информации.

1.4.4. Выполняющих функции по планированию мероприятий по защите информации.

1.4.5. Выполняющих функции по управлению конфигурацией информационной системы и ее системы защиты информации.

2. Контроль безотказного функционирования средств и систем

2.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности

1 или 2 и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1.

2.2. Мероприятия по контролю безотказного функционирования средств и систем должны проводиться на периодической основе и должны быть включены в ежегодный план мероприятий по защите информации.

2.3. Контроль безотказного функционирования должен проводиться в отношении серверного и телекоммуникационного оборудования, каналов связи, средств обеспечения функционирования информационной системы путем периодической проверки работоспособности в соответствии с эксплуатационной документацией (в том числе путем посылки тестовых сообщений и принятия «ответов», визуального контроля, контроля трафика, контроля «поведения» системы или иными методами).

2.4. При обнаружении отказов функционирования должны осуществляться мероприятия по локализации и восстановлению отказавших средств, их тестированию в соответствии с эксплуатационной документацией и планом по действиям сотрудников Института при возникновении нештатных ситуаций, а также регистрация событий, связанных с отказами функционирования, в журнале учета нештатных ситуаций.

3. Резервное копирование

3.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности 1 или 2 и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1 или 2.

3.2. Резервное копирование представляет из себя процесс создания дубликата (копии) информации и (или) программного обеспечения, в том числе программного обеспечения средств защиты информации, на резервном машинном носителе информации (машинном носителе информации, отличном от машинного носителя, на котором хранится информация и (или) программное обеспечение, в том числе программное обеспечение средств защиты информации).

3.3. Информация и программное обеспечение, в том числе программное обеспечение средств защиты информации, подлежащие резервному копированию и периодичность проведения процедуры резервного копирования представлена в таблице 2.

Таблица 2 – Информация и программное обеспечение, в том числе программное обеспечение средств защиты информации, подлежащие резервному копированию

№ п/п	Объект, подлежащий резервному копированию	Периодичность	Ответственный за резервное копирование
1.	БД прикладного программного обеспечения ИС	Еженедельно	Администратор
2.	Настройки	При необходимости	Администратор
3.	Настройки системного, общесистемного и прикладного программного	При необходимости	Ответственные за обеспечение функционирования ИС
4.	Записи регистрации (аудита) событий безопасности	Ежедневно	Администратор системы защиты информации (Администратор

№ п/п	Объект, подлежащий резервному копированию	Периодичность	Ответственный за резервное копирование
			безопасности)
5.	Настройки средств защиты информации	При необходимости	Администратор системы защиты информации (Администратор безопасности)
6.	Полная копия файлов виртуальных дисков и конфигурации виртуальных машин	Ежедневно	Администратор виртуальной машины
7.	СУБД PostgreSQL: Резервные копии БД	Ежедневно	Администратор

3.4. Резервное копирование может выполняться в ручном и в автоматическом режимах. Автоматический режим резервного копирования подразумевает создание дубликатов (копий) информации и программного обеспечения без участия пользователя.

3.5. В случаях, когда резервное копирование в автоматическом режиме не осуществимо, ответственный за резервное копирование должен выполнить процедуру в ручном режиме. Факт выполнения резервного копирования в ручном режиме должен быть зарегистрирован в Журнале резервного копирования и восстановления информации (ПРИЛОЖЕНИЕ № 1).

3.6. Резервное копирование должно быть выполнено таким образом, чтобы была возможность восстановления информации из резервной копии.

3.7. Мероприятия по контролю реализации процедуры резервного копирования должны проводиться на периодической основе и должны быть включены в ежегодный план мероприятий по защите информации.

3.8. Резервное копирование осуществляется на плановой основе с периодичностью, указанной в таблице выше, и внепланово.

3.9. Внеплановое резервное копирование осуществляется в следующих случаях:

– внесены изменения в настройки (конфигурацию) программного обеспечения информационной системы;

– выявлены факты нарушения штатной работы информационной системы;

– по решению сотрудника Института, назначенного ответственным за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных) и ответственным за защиту информации (в отношении государственных информационных систем);

– по решению ответственного за резервное копирование.

3.10. Факт выполнения внепланового резервного копирования в ручном режиме должен быть зарегистрирован в Журнале резервного копирования и восстановления информации.

3.11. Резервные машинные носители информации должны храниться в специально предназначенных помещениях, которые исключают несанкционированный доступ к ним и воздействие внешних факторов, которые могут повлиять на такие носители.

3.12. Защита резервных копий должна обеспечиваться путем реализации необходимых методов, типов и правил разграничения доступа к резервным копиям в соответствии с регламентом управления доступом.

4. Восстановление информации и программного обеспечения

4.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности 1 или 2 и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1 или 2.

4.2. Обеспечение непрерывности функционирования информационной системы достигается путем восстановления информации и программного обеспечения информационной системы в случаях сбоя в течение 1 часа.

4.3. В случае сбоя должны проводиться мероприятия по восстановлению функционирования информационной системы. В зависимости от характера сбоя восстановление функционирования может включать восстановление:

– баз данных прикладного программного обеспечения;

– работоспособности и параметров настроек (конфигурации) системного, общесистемного и прикладного программного обеспечения;

– работоспособности и параметров настроек (конфигурации) программного обеспечения средств защиты информации;

– записей регистрации (аудита) событий безопасности.

4.4. Восстановление функционирования программного обеспечения должно производиться в соответствии с эксплуатационной документацией на программное обеспечение.

4.5. Любое восстановление информации, не вызванное необходимостью экстренного восстановления, которая связана с отказом функционирования информационной системы или ее компонентов, выполняется по решению сотрудника Института, назначенного ответственным за обеспечение безопасности персональных данных (в отношении информационных систем персональных данных) и ответственным за защиту информации (в отношении государственных информационных систем).

4.6. Восстановление информации из резервных копий осуществляется в соответствии с правилами, описанными в системах, с использованием которых осуществлялось создание дубликатов (копий) на резервные машинные носители информации.

4.7. Факт осуществления восстановления функционирования регистрируется ответственными лицами, выполнившими данное действие, в соответствующей рабочей (эксплуатационной) документации на информационную систему и (или) в Журнале резервного копирования и восстановления информации.

5. Контроль предоставляемых вычислительных ресурсов и каналов связи

5.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности 1 или 2.

5.2. Мероприятия по контролю предоставляемых вычислительных ресурсов и каналов связи должны проводиться на периодической основе и должны быть включены в ежегодный план мероприятий по защите информации.

5.3. Контроль должен осуществляться в отношении предоставляемых уполномоченными лицами (провайдерами) услуг по передаче информации.

5.4. Результаты контроля должны быть зафиксированы в соответствующей рабочей (эксплуатационной) документации на информационную систему.

6. Ответственность

6.1. Сотрудники Института, назначенные ответственными за защиту информации и ответственными за обеспечение безопасности персональных данных, и сотрудники Института, выполняющие функции по управлению (администрированию) системой защиты информации, по управлению конфигурацией информационной системы и ее системы защиты информации, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

Приложение № 1
к Регламенту обеспечения доступности в
информационных системах ГАУ ДПО
«Смоленский областной институт развития
образования»

Журнал резервного копирования/восстановления данных

№ п/п	Схема резервного копирования/восстановления данных	Копируемые/восстанавливаемые ресурсы	Хранилище	Дата/время создания копии/восстановления	Фамилия ответственного	Подпись ответственного	Результат резервного копирования/восстановления данных	Комментарий
1	2	3	4	5	6	7	8	9

Приложение № 11
к приказу ГАУ ДПО «Смоленский областной
институт развития образования»
от «21» 10 2024г. №201-од

Регламент защиты среды виртуализации в информационных системах ГАУ ДПО «Смоленский областной институт развития образования»

1. Общие положения

1.1. Настоящий Регламент разработан с целью установления ГАУ ДПО «Смоленский областной институт развития образования» (далее – Институт) общих правил, требований и процедур защиты среды виртуализации информационных систем (далее – ИС) Института и информации, в том числе персональных данных.

1.2. Положения настоящего Регламента должны применяться в отношении информационных систем, в которых применяются технологии виртуализации.

1.3. Меры защиты информации, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты информации, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты информации
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей

1.4. Состав мер определен на основании установленного класса защищенности информационной системы, уровня защищенности персональных данных и структурно-функциональных характеристик ИС Института.

1.5. Регламент предназначен для сотрудников Института:

1.5.1. Назначенных ответственными за обеспечение безопасности персональных данных.

1.5.2. Назначенных ответственными за защиту информации.

1.5.3. Выполняющих функции по управлению (администрированию) системой защиты информации.

1.5.4. Выполняющих функции по планированию мероприятий по защите информации.

1.5.5. Выполняющих функции по управлению конфигурацией информационной системы и ее системы защиты информации.

2. Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре

2.1. В информационной системе должны обеспечиваться идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре в соответствии с регламентом идентификации и аутентификации.

2.2. При реализации мер по идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре должны обеспечиваться:

– идентификация и аутентификация администраторов управления средствами виртуализации;

– идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам доступа в виртуальной инфраструктуре;

– блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

– защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерного доступа к ней, уничтожения или модифицирования;

– защита аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющими на это полномочий;

– идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления параметрами аппаратного обеспечения виртуальной инфраструктуры.

2.3. Внутри развернутых на базе виртуальной инфраструктуры виртуальных машин должна быть также обеспечена реализация мер по идентификации и аутентификации субъектов и объектов доступа в соответствии регламентом идентификации и аутентификации.

3. Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре

3.1. В информационной системе должно обеспечиваться управление доступом субъектов доступа к объектам доступа, в том числе внутри виртуальных машин, в соответствии с регламентом управления доступом.

3.2. В качестве объектов доступа в виртуальной инфраструктуре необходимо, как минимум, рассматривать программное обеспечение управления виртуальной инфраструктурой, гипервизор, хостовую операционную систему (если применимо), виртуальные машины, программную среду виртуальных машин (в том числе их операционные системы и программное обеспечение), виртуальные контейнеры (зоны), виртуализированное программное обеспечение (виртуальные машины с предустановленным программным обеспечением, предназначенным для выполнения

определенных функций в виртуальной инфраструктуре), средства защиты информации, используемые в рамках виртуальных машин и виртуальной инфраструктуры в целом.

3.3. При реализации мер по управлению доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре должно обеспечиваться:

– контроль доступа субъектов доступа к средствам управления компонентами виртуальной инфраструктуры;

– контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды;

– управление доступом к виртуальному аппаратному обеспечению информационной системы, являющемуся объектом доступа;

– контроль запуска виртуальных машин на основе заданных оператором правил (режима запуска, типа используемого носителя и иных правил);

– разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к объектам доступа, расположенным внутри виртуальных машин, в соответствии с правилами разграничения доступа пользователей данных виртуальных машин;

– разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к ресурсам информационной системы, размещенным за пределами виртуальных машин, в соответствии с правилами разграничения доступа, принятыми в информационной системе в целом.

4. Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре

4.1. Положения данного раздела должны применяться только в отношении государственных информационных систем независимо от установленного класса защищенности и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1, 2 или 3.

4.2. В информационной системе должна обеспечиваться регистрация событий безопасности в виртуальной инфраструктуре в соответствии с регламентом регистрации событий безопасности.

4.3. В виртуальной инфраструктуре должны подлежать регистрации следующие события:

– запуск (завершение) работы компонентов виртуальной инфраструктуры;

– доступ субъектов доступа к компонентам виртуальной инфраструктуры;

– изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения;

– изменения правил разграничения доступа к компонентам виртуальной инфраструктуры.

5. Управление потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры

5.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности 1 или 2.

5.2. В информационной системе должно осуществляться управление потоками информации между компонентами виртуальной инфраструктуры и по периметру виртуальной инфраструктуры в соответствии с разделами 3 и 4 регламента защиты информационной системы, ее средств, систем связи и передачи данных.

5.3. При реализации мер по управлению потоками информации между компонентами виртуальной инфраструктуры должно обеспечиваться:

– фильтрация сетевого трафика между компонентами виртуальной инфраструктуры, в том числе между внешними по отношению к серверу виртуализации сетями и внутренними по отношению к серверу виртуализации сетями, в том числе при организации сетевого обмена с сетями связи общего пользования;

– обеспечение доверенных канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и средствами защиты информации (функциями безопасности);

– контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях гипервизора, хостовой операционной системы, по составу, объёму и иным характеристикам;

– отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры гипервизора, хостовой операционной системы, виртуальной вычислительной сети;

– обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;

– обеспечение изоляции потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры (гипервизором, хостовой операционной системой), и сетевых потоков виртуальной вычислительной сети;

– семантический и статистический анализ сетевого трафика виртуальной вычислительной сети.

6. Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных

6.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности 1 или 2 и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1 или 2.

6.2. В виртуальной инфраструктуре должно обеспечиваться управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.

6.3. Допустимые места размещения файлов-образов виртуальных машин (контейнеров) информационных систем Института и их исполнения представлены в Приложении № 1 к настоящему Регламенту.

6.4. Внесение изменений в установленные настоящим Регламентом правила размещения и исполнения виртуальных машин (контейнеров) должно осуществляться сотрудниками Института, выполняющими функции по управлению конфигурацией информационной системы и ее системы защиты информации.

7. Контроль целостности виртуальной инфраструктуры и ее конфигураций

7.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности 1 или 2 и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1 или 2.

7.2. Мероприятия по контролю целостности виртуальной инфраструктуры и ее конфигураций должны проводиться на периодической основе и должны быть включены в ежегодный план мероприятий по защите информации.

7.3. В ходе проведения мероприятия по контролю целостности виртуальной инфраструктуры и ее конфигураций должно осуществляться:

– контроль целостности компонентов, критически важных для функционирования хостовой операционной системы, гипервизора, гостевых операционных систем и (или) обеспечения безопасности обрабатываемой в них информации (загрузчика, системных файлов, библиотек операционной системы и иных компонентов);

– контроль целостности состава и конфигурации виртуального оборудования;

– контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин;

– контроль целостности файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем (контроль файлов-образов должен проводиться во время, когда файлы-образы не задействованы).

7.4. Результаты контроля должны быть зафиксированы в соответствующей рабочей (эксплуатационной) документации на информационную систему.

8. Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры

8.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности 1 или 2 и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1 или 2.

8.2. В виртуальной инфраструктуре информационной системы должно обеспечиваться резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры и каналов связи внутри виртуальной инфраструктуры в соответствии с регламентом обеспечения доступности.

8.3. При реализации мер по резервному копированию данных, резервированию технических средств, программного обеспечения виртуальной инфраструктуры должно обеспечиваться:

– определение мест хранения резервных копий виртуальных машин

(контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре;

– резервное копирование виртуальных машин (контейнеров);

– резервное копирование данных, обрабатываемых в виртуальной инфраструктуре;

– резервирование программного обеспечения виртуальной инфраструктуры;

– резервирование каналов связи, используемых в виртуальной инфраструктуре;

– периодическая проверка резервных копий и возможности восстановления виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре с использованием резервных копий.

8.4. Мероприятия по периодической проверке резервных копий и возможности восстановления виртуальных машин (контейнеров) и данных с использованием резервных копий должны проводиться на периодической основе и должны быть включены в ежегодный план мероприятий по защите информации. Результаты проверки должны быть зафиксированы в соответствующей рабочей (эксплуатационной) документации на информационную систему.

9. Антивирусная защита в виртуальной инфраструктуре

9.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности 1 или 2 и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1, 2 или 3.

9.2. В виртуальной инфраструктуре информационной системы должны использоваться средства антивирусной защиты информации в соответствии с регламентом антивирусной защиты.

9.3. Антивирусная защита виртуальной инфраструктуры должна обеспечивать:

– проверку наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;

– проверку наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.

10. Разбиение виртуальной инфраструктуры на сегменты

10.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности 1 или 2 и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1, 2 или 3.

10.2. В виртуальной инфраструктуре информационной системы должно обеспечиваться разбиение на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей в соответствии с разделом «Разбиение информационной системы на сегменты» регламента защиты информационной системы, ее средств, систем связи и передачи данных.

10.3. Принципы разбиения виртуальной инфраструктуры на сегменты должны определяться в проектной документации на систему защиты информации с учетом

функциональных и технологических особенностей процесса обработки информации и анализа угроз безопасности информации.

11. Ответственность

11.1. Сотрудники Института, назначенные ответственными за защиту информации и ответственными за обеспечение безопасности персональных данных, и сотрудники Института, выполняющие функции по управлению (администрированию) системой защиты информации, по планированию мероприятий по защите информации, по управлению конфигурацией информационной системы и ее системы защиты информации, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

Приложение № 1
к регламенту защиты среды виртуализации в
информационных системах ГАУ ДПО
«Смоленский областной институт развития
образования»

Разрешенные места размещения и исполнения виртуальных машин (контейнеров)

№ п/п	Наименование файла-образа виртуальной машины (контейнера)	Разрешенные места размещения файла-образа виртуальной машины (контейнера)	Разрешенные места исполнения виртуальной машины (контейнера)
1.	**Государственная информационная система «Образование»**		
1.1.	Сервер le-aisko-01	server_virt	server_virt

Приложение № 12
к приказу ГАУ ДПО «Смоленский областной
институт развития образования»
от «21» 10 2024г. №201-од

Регламент защиты технических средств в информационных системах ГАУ ДПО «Смоленский областной институт развития образования»

1. Общие положения

1.1. Настоящий Регламент разработан с целью установления ГАУ ДПО «Смоленский областной институт развития образования» (далее – Институт) общих правил, требований и процедур защиты технических средств информационных систем (далее – ИС) Института и информации, в том числе персональных данных.

1.2. Меры защиты информации, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты информации, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры 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 и помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

1.3. Состав мер определен на основании установленного класса защищенности информационной системы, уровня защищенности персональных данных и структурно-функциональных характеристик ИС Института.

1.4. Регламент предназначен для сотрудников Института:

1.4.1. Назначенных ответственными за обеспечение безопасности персональных данных.

1.4.2. Назначенных ответственными за защиту информации.

1.4.3. Выполняющих функции по управлению конфигурацией информационной системы и ее системы защиты информации.

2. Организация контролируемой зоны

2.1. Под организацией контролируемых зон подразумевается определение начальником Института границ контролируемых зон.

2.2. Границами контролируемой зоны могут являться периметр охраняемой территории, ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.

2.3. При определении границ контролируемых зон необходимо рассматривать пространство (территорию, здание, часть здания), в пределах которой постоянно размещаются:

– стационарные технические средства;

– средства защиты информации;

– средства обеспечения функционирования.

3. Управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены

3.1. Управление физическим доступом предусматривает:

– определение перечня помещений, в которых размещены информационные системы Института. Перечень утверждается начальником Института;

– определение порядка доступа сотрудников Института в помещения, в которых осуществляется обработка защищаемой информации и размещены информационные системы. Порядок утверждается начальником Института;

– санкционирование физического доступа;

– учет доступа.

3.2. Управление физическим доступом может достигаться за счет:

– оснащения входных дверей помещений, в которых расположены технические средства и устройства информационной системы, замками;

– постоянным закрытием входных дверей помещений, в которых расположены технические средства и устройства информационной системы, на замок и их открытием только для санкционированного прохода;

– внедрением контрольно-пропускного и внутриобъектового режима (доступ посетителей на территорию Института осуществляется только при наличии пропуска и документа, удостоверяющего личность);

– организацией доступа к информационным ресурсам по заявке, согласованной в соответствии с пропускным внутриобъектовым режимом;

– предоставления доступа в помещения, в которых размещены серверные компоненты информационной системы и обеспечивающие их функционирование устройства, строго определенному кругу лиц, осуществляющему их техническое обслуживание и сопровождение;

– ограничения нахождения посетителей и других лиц имеющих право разового доступа на территории Института. Нахождение таких лиц допускается только в присутствии лиц, имеющих право постоянного доступа на территорию Института;

– ознакомления лиц, имеющих право постоянного доступа в помещения, в которых размещены информационные системы Института, с локальными нормативными актами Института в области обеспечения безопасности информации;

– предоставление доступа в помещения, в которых размещены информационные системы, только тем лицам, которым указанный доступ необходим в рамках исполнения должностных обязанностей или обязанностей, предусмотренных договорами (соглашениями);

– фиксированием факта разового доступа лиц в помещения, в которых размещены информационные системы.

4. Размещение устройств вывода (отображения) информации

4.1. В качестве устройств вывода (отображения) информации рассматриваются:

– мониторы автоматизированных рабочих мест пользователей;

– мониторы консолей управления технических средств (серверов, телекоммуникационного оборудования и иных технических средств);

– печатающие устройства.

4.2. При размещении данных устройств вывода (отображения) информации следует исключать возможность несанкционированного просмотра выводимой на них информации как из-за пределов помещения, в которых размещено устройство, так и в пределах этих помещений. С этой целью не следует размещать устройства вывода (отображения, печати) информации напротив:

– оконных проемов;

– входных дверей;

– технологических отверстий;

– в коридорах, холлах;

– в иных местах, доступных для несанкционированного просмотра.

5. Ответственность

5.1. Сотрудники Института, назначенные ответственными за защиту информации и ответственными за обеспечение безопасности персональных данных, и сотрудники Института, выполняющие функции по управлению конфигурацией информационной системы и ее системы защиты информации, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

Приложение № 13
к приказу ГАУ ДПО «Смоленский областной
институт развития образования»
от «21» 10 2024г. № 201-од

Регламент защиты информационных систем ГАУ ДПО «Смоленский областной институт развития образования», их средств, систем связи и передачи данных

1. Общие положения

1.1. Настоящий Регламент разработан с целью установления ГАУ ДПО «Смоленский областной институт развития образования» (далее – Институт) общих правил, требований и процедур защиты информационных систем (далее – ИС) Института, ее средств, систем связи и передачи данных.

1.2. Меры защиты информации, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты информации, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты информации
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы
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.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода
ЗИС.8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в

Условное обозначение и номер меры	Меры защиты информации
	процессе обработки информации
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы
ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями
ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения

1.3. Состав мер определен на основании установленного класса защищенности информационной системы, уровня защищенности персональных данных и структурно-функциональных характеристик ИС Института.

1.4. Регламент предназначен для сотрудников Института:

1.4.1. Назначенных ответственными за обеспечение безопасности персональных данных.

1.4.2. Назначенных ответственными за защиту информации.

1.4.3. Выполняющих функции по управлению (администрированию) системой защиты информации.

1.4.4. Выполняющих функции по планированию мероприятий по защите информации.

1.4.5. Выполняющих функции по управлению конфигурацией информационной системы и ее системы защиты информации.

2. Разделение функций в информационной системе

2.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности 1 или 2 и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1.

2.2. В информационной системе должно быть обеспечено разделение функций (функциональных возможностей) по:

– управлению (администрированию) информационной системой;

– управлению (администрированию) системой защиты информации информационной системы;

– обработке информации.

2.3. Разделение функций (функциональных возможностей) должно быть выполнено в отношении каждой информационной системы Института в ходе реализации системы разграничения доступа и должно быть отражено в соответствующей эксплуатационной (рабочей) документации.

2.4. В качестве функциональных возможностей по управлению (администрированию) информационной системы следует рассматривать функции:

– по управлению базами данных, прикладным программным обеспечением, телекоммуникационным оборудованием, рабочими станциями и серверами;

– иные функции, требующие высоких привилегий.

2.5. В качестве функциональных возможностей по управлению (администрированию) системой защиты информации информационной системы следует рассматривать функции:

– по управлению функциями безопасности, реализуемые программными и программно-аппаратными средствами информационной системы;

– по управлению средствами защиты информации;

– иные функции, требующие высоких привилегий.

2.6. Разделение функциональных возможностей должно быть выполнено одним или комбинацией следующих способов:

2.7. Разделение на физическом уровне путем выделения части программно-технических средств (автоматизированных рабочих мест, серверов и т.д.).

2.8. Разделение на логическом уровне путем:

– распределения программно-аппаратных средств в различные домены.

– выделения сетевых адресов;

– выделения каналов управления.

3. Защита информации при ее передаче по каналам связи

3.1. При передаче информации по каналам связи, выходящим за пределы контролируемой зоны, должна быть обеспечена защита информации от раскрытия, модификации и навязывания (ввода ложной информации).

3.2. Защита информации при ее передаче по каналам связи должна обеспечиваться одним или комбинацией из следующих способов:

– защита каналов связи от несанкционированного физического доступа (подключения) к ним;

– применение средств криптографической защиты информации.

3.3. Для защиты информации криптографическими методами должны использоваться программные или программно-аппаратные средства, прошедшие оценку соответствия в форме обязательной сертификации.

4. Управление сетевыми потоками

4.1. В информационной системе должно осуществляться управление сетевыми потоками при передаче информации между устройствами, сегментами, включающее:

– фильтрацию сетевых потоков в соответствии с правилами управления потоками;

– разрешение передачи информации только по разрешенному маршруту;

– изменение (перенаправление) маршрута передачи информации (в установленных Институтом случаях);

– запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи (в установленных Институтом случаях).

4.2. Управление сетевыми потоками должно обеспечивать разрешенный маршрут прохождения информации между устройствами, сегментами информационной системы, а также между информационными системам или при взаимодействии с информационно-телекоммуникационными сетями провайдеров,

предоставляющих услуги связи или сетями связи общего пользования на основе правил управления сетевыми потоками.

5. Запрет несанкционированной удаленной активации периферийных устройств

5.1. Положения данного раздела должны применяться только в отношении государственных информационных систем независимо от установленного класса защищенности.

5.2. В информационной системе должны быть запрещены операции, связанные с удаленной активацией периферийных устройств.

5.3. Запрет несанкционированной удаленной активации должен осуществляться в отношении всех периферийных устройств ввода (вывода) информации, которые имеют возможность управления (запуска, включения, выключения) через компоненты программного обеспечения, установленные на рабочем месте пользователя, коммуникационных сервисов сторонних лиц (провайдеров) (ICQ, Skype и иные сервисы).

5.4. В качестве периферийных устройств следует, как минимум, рассматривать

– видеокамеры;

– микрофоны;

– иные периферийные устройства ввода (вывода) информации.

5.5. Запрет несанкционированной удаленной активации должен осуществляться через физическое исключение такой возможности и (или) программным способом.

5.6. Исключительные случаи, при которых допускается возможность удаленной активации периферийных устройств в Институте не определены.

6. Использование технологий мобильного кода

6.1. Положения данного раздела должны применяться только отношении государственных информационных систем с установленным классом защищенности 1 или 2.

6.2. В информационной системе должно быть исключено использование технологий мобильного кода (использование Java, JavaScript, ActiveX, PDF, Postscript, Flash-анимация и VBScript) на всех технических средствах за исключением разрешенных мест распространения (серверы информационной системы) и использования мобильного кода (автоматизированные рабочие места, мобильные технические средства информационной системы).

6.3. На разрешенных местах распространения и использования мобильного кода должны быть предприняты меры защиты информации, направленные на регистрацию событий, связанных с использованием технологии мобильного кода.

6.4. Мероприятия по контролю использования технологий мобильного кода на технических средствах информационных систем должны проводиться на периодической основе и должны быть включены в ежегодный план мероприятий по защите информации.

7. Использование технологий передачи речи и видеоинформации

7.1. Положения данного раздела должны применяться только отношении государственных информационных систем с установленным классом защищенности 1 или 2.

7.2. В информационной системе должно быть исключено использование технологий (сервисов) передачи речи и видеоинформации на всех технических средствах за исключением разрешенных мест использования. Перечень разрешенных мест использования технологий (сервисов) передачи речи и видеоинформации должны определяться в проектной документации на систему защиты информации.

7.3. На разрешенных местах использования должны быть предприняты меры защиты информации, направленные на регистрацию событий, связанных с использованием технологии исключения удаленной конфигурации (настройки параметров устройства передачи речи и устройства передачи видеоинформации).

7.4. Мероприятия по контролю использования технологий (сервисов) передачи речи и видеоинформации на технических средствах информационных систем должны проводиться на периодической основе и должны быть включены в ежегодный план мероприятий по защите информации.

8. Исключение возможности отрицания пользователем факта отправки и получения информации

8.1. Положения данного раздела должны применяться только отношении государственных информационных систем с установленным классом защищенности 1 или 2.

8.2. В информационной системе должна быть исключена возможность отрицания пользователем факта отправки информации другому пользователю и ее получения от другого пользователя.

8.3. Для исключения возможности отрицания на технических средствах информационной системы должны быть реализованы меры защиты информации, направленные на регистрацию событий, связанных с отправкой информации другому пользователю и ее получением.

8.4. Перечень объектов и типов информации, для которых требуется обеспечение неотказуемости, должны определяться в проектной документации на систему защиты информации.

9. Обеспечение подлинности сетевых соединений

9.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности 1 или 2 и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1 или 2.

9.2. В информационной системе должно осуществляться обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (защита от атак типа «человек посередине»).

9.3. Принципы обеспечения подлинности сетевых соединений должны определяться в проектной документации на систему защиты информации с учетом

функциональных и технологических особенностей процесса обработки информации и анализа угроз безопасности информации.

10. Защита неизменяемых данных

10.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности 1 или 2 и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1 или 2.

10.2. В информационной системе должно обеспечиваться управление доступом к неизменяемым данным в соответствии с регламентом управления доступом. К данным, не подлежащим изменению в процессе обработки информации, (неизменяемым данным) в информационной системе следует, как минимум относить:

– архивные файлы;
– параметры настроек средств защиты информации;
– параметры настроек программного обеспечения.

11. Разбиение информационной системы на сегменты

11.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности 1 или 2 и в отношении информационных систем персональных данных с установленным уровнем защищенности персональных данных 1 или 2.

11.2. С целью построения многоуровневой (эшелонированной) систем защиты информации должно осуществляться сегментирование. Сегментирование должно быть направлено на снижение вероятности реализации угроз и (или) их локализацию в рамках одного сегмента информационной системы. Принципы сегментирования информационных систем должны определяться в проектной документации на систему защиты информации с учетом функциональных и технологических особенностей процесса обработки информации и анализа угроз безопасности информации.

12. Защита от угроз отказа в обслуживании (DOS, DDOS-атак)

12.1. Положения данного раздела должны применяться только отношении государственных информационных систем с установленным классом защищенности 1 или 2.

12.2. В информационной системе должна обеспечиваться защита от угроз безопасности информации, направленных на отказ в обслуживании.

12.3. Защита от угроз безопасности информации, направленных на отказ в обслуживании, может осуществляться посредством реализации в информационной системе мер по управлению сетевыми потоками и повышенными характеристиками производительности телекоммуникационного оборудования и каналов передачи совместно с резервированием информации и технических средств, программного обеспечения, каналов передачи информации.

12.4. Принципы защиты от угроз безопасности информации, направленных на отказ в обслуживании, должны определяться в проектной документации на систему

защиты информации с учетом функциональных и технологических особенностей процесса обработки информации и анализа угроз безопасности информации.

13. Защита сетевого периметра

13.1. Положения данного раздела должны применяться только в отношении государственных информационных систем с установленным классом защищенности 1 или 2.

13.2. В информационной системе должна обеспечиваться защита сетевого периметра при ее взаимодействии с иными информационными (автоматизированными) системами и информационно-телекоммуникационными сетями.

13.3. Физической границей сетевого периметра следует рассматривать оборудование, обеспечивающее физическое соединение сетей электросвязи Института или подразделений Института (филиалов, представительств и т.д.) с информационно-телекоммуникационными сетями провайдеров, предоставляющих услуги связи, или сетями связи общего пользования.

13.4. Логической границей сетевого периметра информационной системы следует рассматривать оборудование, обеспечивающее разделение сетей электросвязи Института или подразделений Института (филиалов, представительств и т.д.) на самостоятельные разделяемые среды передачи данных (обеспечивается логическое объединение узлов сети электросвязи, при котором обмен данными на уровне звена данных модели взаимосвязи открытых систем возможен только между этими узлами сети электросвязи).

13.5. Защита периметра на физической границе сетевого периметра должна обеспечиваться за счет:

– использования в качестве оборудования, обеспечивающего физическое соединение, программно-аппаратного средства, прошедшего оценку на соответствие требованиям по безопасности в формах обязательной сертификации;

– управления сетевыми потоками (входящими в сеть электросвязи Института и исходящими из нее).

13.6. Защита периметра на логической границе сетевого периметра должна обеспечиваться за счет:

– использования в качестве оборудования, обеспечивающего разделение сети электросвязи Института на самостоятельные разделяемые среды передачи данных программных или программно-аппаратных средств, прошедших оценку на соответствие требованиям по безопасности в форме обязательной сертификации;

– управления сетевыми потоками (входящими в сеть электросвязи Института и исходящими из нее).

13.7. Управление сетевыми потоками на физической и (или) логической границе должно осуществляться в соответствии с разделом «Управление сетевыми потоками» настоящего Регламента.

14. Управление сетевыми соединениями

14.1. Положения данного раздела должны применяться только отношении государственных информационных систем с установленным классом защищенности 1 или 2.

14.2. В информационной системе должно осуществляться прекращение сетевых соединений по их завершении и (или) по истечении заданного временного интервала неактивности сетевого соединения.

15. Ответственность

15.1. Сотрудники Института, назначенные ответственными за защиту информации и ответственными за обеспечение безопасности персональных данных, и сотрудники Института, выполняющие функции по управлению (администрированию) системой защиты информации, по планированию мероприятий по защите информации, по управлению конфигурацией информационной системы и ее системы защиты информации, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

Лист ознакомления
с мерами по защите информации в информационных системах ГАУ ДПО
«Смоленский областной институт развития образования»

№ п/п	ФИО	Должность	Дата	Подпись
1	Клейтман Н.В.	начальник Центра	22.10.24	[signature]
2	Петрачкова Е.Л.	методист	22.10.24	[signature]
3	Шматов Е.А.	методист	22.10.24	[signature]
4	Забелин	зав. отделом	22.10.24	[signature]
5.	Зелезова М.Н.	методист	23.10.2024	[signature]
6.	Пушкарева К.А.	методист	23.10.2024	[signature]
7.	Ходенкова М.А.	методист	22.10.2024	[signature]
8.	Катренин В.В.	методист	22.10.2024	[signature]
9.	Чужакина Е.В.	методист	23.10.24	Чужакина
10.	Кулешова А.В.	методист	23.10.24	[signature]
11	Семенова М.В.	начальник РИБЦ	23.10.24	[signature]
12	Кудрицкий	методист ЦО	23.10.24	[signature]
13.	Воробьёва Ю.В.	вед. бухгалтер	23.10.24	[signature]
14.	Нестова О.И.	главный бухгалтер	23.10.2024	[signature]
15.	Гуленко Л.Н.	кладовщик	23.10.2024	[signature]