

муниципальное бюджетное учреждение  
«Олонецкий национальный музей карелов-ливвиков  
им. Н. Г. Прилукина»

П Р И К А З

№ 46/2

от 01 апреля 2026 года

**Об утверждении модели актуальных угроз безопасности персональных данных в информационных системах.**

**ПРИКАЗЫВАЮ:**

1. Утвердить модель актуальных угроз безопасности персональных данных в информационных системах.
2. Организатору экскурсий Сарычевой Екатерине Сергеевне разместить Модель на официальном сайте Музея.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор



 / Н. В. Николаева /

Утверждено  
Приказом № 46/2  
от 01.04.2026 г.

**МОДЕЛЬ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ  
ПЕРСОНАЛЬНЫХ ДАННЫХ  
В ИНФОРМАЦИОННЫХ СИСТЕМАХ  
МБУ «Олонецкий национальный музей»**

**ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

**Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники.

**Безопасность персональных данных** – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**Блокирование персональных данных**- временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**Вирус (компьютерный, программный)** – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**Доступ в операционную среду компьютера (информационной системы персональных данных)** - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

**Доступ к информации** – возможность получения информации и ее использования.

**Закладочное устройство** - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Источник угрозы безопасности информации** – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Нарушитель безопасности персональных данных** – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

**Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

**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.

**Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

**Побочные электромагнитные излучения и наводки** – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**Пользователь информационной системы персональных данных** – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

**Правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц

**Программная закладка** – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

**Программное (программно-математическое) воздействие** – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

**Распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц

**Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

**Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

**Утечка (защищаемой) информации по техническим каналам** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

**Уязвимость ИСПДн** – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности ПДн.

## ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ – автоматизированное рабочее место;

ИСПДн – информационная система персональных данных;

НСД – несанкционированный доступ;

ОБПДн – обеспечение безопасности персональных данных;

ОС – операционная система;

ПДн – персональные данные;

СЗИ – средство защиты информации;

СЭУПИ – специальные электронные устройства перехвата информации;

УБПДн – угрозы безопасности персональных данных.

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

Модель актуальных угроз МБУ «Олонецкий национальный музей» (далее Оператор) разработана в соответствии с нормативными документами ФСТЭК России:

- Базовая модель безопасности персональных данных при их обработке в информационных системах персональных данных;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Модель угроз содержит описание возможных угроз безопасности персональных данных и расчет актуальных угроз для ИСПДн Оператора.

Модель угроз направлена на определение возможных каналов утечки, путем анализа защищенности ИСПДн Оператора.

Под угрозами безопасности ПДн при их обработке в ИСПДн понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

В соответствии со статьей 19 Федерального закона №152-ФЗ от 27 июля 2006 г. «О персональных данных», ПДн должны быть защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а так же от иных неправомерных действий. Угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн и (или) потребителей, пользующихся услугами, предоставляемыми ИСПДн в соответствии с ее назначением, так и со специально осуществляемыми неправомерными действиями криминальных сообществ, отдельных организаций и граждан, а также иными источниками угроз.

Угрозы безопасности ПДн могут быть реализованы за счет утечки ПДн по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа с

использованием соответствующего программного обеспечения.

Угрозы безопасности ПДн, обрабатываемых в ИСПДн Оператора, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПДн. Кроме того, Модель угроз может быть пересмотрена по решению оператора на основе периодически проводимых им анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений ИСПДн, а также по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПДн при их обработке в информационной системе.

## 2. ОПИСАНИЕ ИСПДН

ИСПДн Оператора состоит из следующих программных компонентов:

- 1СПредприятие: Бухгалтерия (версия8.3);
- 1С Зарплата (версия8.3);
- СБИС (Saby repost, Saby docs)

ИСПДн предназначены для автоматизации обработки информации:

- ПДн сотрудников Оператора, физические лица по договорам гражданско-правового характера и самозанятые граждане Оператора.

В ИСПДн не обрабатываются специальные, биометрические и общедоступные персональные данные. Таким образом, ИСПДн является системой, обрабатывающей иные категории персональных данных.

В ИСПДн одновременно обрабатываются персональные данные менее чем 100 000 субъектов персональных данных.

Все информационные системы Оператора, кроме ИСПДн Сбис, являются локальными информационными системами, поскольку входящие в ее состав технические средства обработки информации размещены в пределах одного здания. Контролируемой зоной ИСПДн являются рабочие помещения Оператора. Границами контролируемых зон являются стены, двери, окна и межэтажные перекрытия помещений.

В качестве среды передачи данных используется локальная сеть Оператора. ИСПДн имеет следующие характеристики:

- Категория обрабатываемых ПДн: 4 категория – иные категории.
- Уровень защищенности данных четвертый
- Режим обработки персональных данных: многопользовательский с разграничением прав доступа пользователей;
- цель создания ИСПДн (цель обработки ПДн): обеспечение рабочего процесса;
- вид обработки ПДн: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача),

уничтожение ПДн

Доступ на территорию учреждения круглосуточно контролируется охраной, видеонаблюдение окружающей территории.

### 3. ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИСПДн

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн.

Актуальность угрозы определяется следующими параметрами:

- Уровень исходной защищенности ИСПДн;
- Частота (вероятность)реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн. Характеристики ИСПДн «Бухгалтерия и кадры» приведены в таблице:

№	Параметр	Значение	Уровень защищенности
1	Территориальное размещение	Локальная ИСПДн, развернутая в пределах одного здания	высокий
2	Наличие соединений с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования	средний
3	Встроенные (легальные) операции с записями баз персональных данных	запись, удаление, сортировка	средний
4	Разграничение доступа к персональным данным	ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн	средний

Значению уровня защищенности «Высокий» соответствуют 1 характеристики, значению уровня «Средний» -3 характеристики, значению уровня «Низкий»-0 характеристик. Таким образом, числовой коэффициент исходной защищенности ИСПДн Оператора соответствует значению 3 (средняя).

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

- *Маловероятно* – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

– *низкая вероятность* – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

– *средняя вероятность* - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

– *высокая вероятность* - объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент  $Y_2$ , а именно:

- 0 для маловероятной угрозы;
- 2 для низкой вероятности угрозы;
- 5 для средней вероятности угрозы;
- 10 для высокой вероятности угрозы.

### ТАБЛИЦА УГРОЗ БЕЗОПАСНОСТИ

Наименование угрозы	Вероятность ( $Y_2$ )	Реализуемость ( $Y$ )	Опасность	Актуальность
<b>УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ</b>				
Угрозы утечки акустической (речевой) информации	маловероятно (0)	низкая	низкая	неактуальная
Угрозы утечки видовой информации	средняя вероятность(5)	средняя	низкая	актуальная
<b>УГРОЗЫ НСД К ПДн ,ОБРАБАТЫВАЕМЫМ НА АВТОМАТИЗИРОВАННОМ РАБОЧЕМ МЕСТЕ</b>				
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода(BIOS), перехват управления загрузкой	маловероятно(0)	низкая	низкая	неактуальная

Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	маловероятно (0)	низкая	низкая	неактуальная
Угрозы внедрения вредоносных программ	Маловероятно (0)	низкая	низкая	неактуальная

УГРОЗЫ ИЗ ВНЕШНИХ СЕТЕЙ				
Угрозы выявления паролей	маловероятно (0)	низкая	низкая	неактуальная
Угрозы удаленного запуска приложений	маловероятно (0)	низкая	низкая	неактуальная
Угрозы внедрения по сети вредоносных программ	маловероятно (0)	низкая	низкая	неактуальная

#### 4. МОДЕЛЬ ВЕРОЯТНОГО НАРУШИТЕЛЯ

По наличию права постоянного или разового доступа в ИСПДн нарушители подразделяются на два типа:

- нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена – внешние нарушители;
- нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн – внутренние нарушители.

Внешними нарушителями могут быть:

- криминальные структуры;
- недобросовестные партнеры;
- внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

- осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
- осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования;
- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны.

#### КАТЕГОРИИ НАРУШИТЕЛЕЙ

№	Описание	Нарушитель может	Возможный нарушитель
1	Лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, Обеспечивающие нормальное функционирование ИСПДн.	<ul style="list-style-type: none"><li>– иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн;</li><li>– располагать именами и вести выявление паролей зарегистрированных пользователей;</li><li>– изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.</li></ul>	Сотрудники, не участвующие в обработке ПДн

2	Зарегистрированные пользователи ИСПДн, осуществляющие Ограниченный доступ к ресурсам ИСПДн с рабочего места.	<ul style="list-style-type: none"> <li>- Обладает всеми возможностями лиц первой категории;</li> <li>- Знает по меньшей мере одно легальное имя доступа;</li> <li>- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;</li> <li>- располагает конфиденциальными данными, к которым имеет доступ.</li> </ul>	Сотрудники, обрабатывающие ПДн
3	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн	<ul style="list-style-type: none"> <li>- обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения;</li> <li>- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.</li> </ul>	Системный администратор ИСПДн