Частная модель угроз безопасности персональных данных в информационных системах в МБДОУ №44

2023

1. СОКРАЩЕНИЯ

В настоящем документе применяются следующие обозначения и сокращения:

АС	- автоматизированная система;
АСЗИ	- автоматизированная система в защищенном исполнении;
АРМ	- автоматизированное рабочее место;
ВТСС	- вспомогательные технические средства и системы;
ИСПДн	- информационная система персональных данных;
КЗ	- контролируемая зона;
ЛВС	- локальная вычислительная сеть;
МЭ	- межсетевой экран;
НДВ	- недокументированные (недекларированные) возможности
НСД	- несанкционированный доступ, несанкционированные действия;
ОС	- операционная система;
ПДн	- персональные данные;
ПК	- программный комплекс;
ПО	- программное обеспечение;
ПЭМИН	- побочные электромагнитные излучения и наводки;
СВТ	- средства вычислительной техники;
СЗИ	- средство защиты информации;
СКЗИ	- средства криптографической защиты информации;
СФ	- среда функционирования СКЗИ;
СВТ	- средства вычислительной техники;
ТКУИ	- технический канал утечки информации;
ЭП	- электронная подпись.

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. **Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.

1.2. **Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

1.3. **Автоматизированная система в защищенном исполнении** – автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и (или) иных нормативных документов по защите информации.

1.4. **Автоматизированное рабочее место** – программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида.

1.5. **Аутентификация отправителя данных** – подтверждение того, что отправитель полученных данных соответствует заявленному**.**

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

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

1.8. **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.

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

1.10. **Вспомогательные технические средства и системы** – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

1.11. **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.

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

1.13. **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).

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

1.15. **Идентификация** – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

1.17. **Информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

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

1.19. **Контролируемая зона** – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

1.20. **Межсетевой экран** – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

1.21. **Модель нарушителя** – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

1.22. **Модель угроз –** перечень возможных угроз.

1.23. **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.

1.24. **Недокументированные (недекларированные) возможности** – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

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

1.26. **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.

1.27. **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

1.28. **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.

1.29. **Объект информатизации** – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

1.30. **Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.31. **Операционная система** – совокупность системных программ, предназначенная для обеспечения определенного уровня эффективности системы обработки информации за счет автоматизированного управления ее работой и предоставляемого пользователю определенного набора услуг.

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

1.33. **Перехват (информации)** – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

1.34. **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.

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

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

1.37. **Программная закладка** – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

1.38. **Программное обеспечение** – совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

1.39. **Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.40. **Ресурс информационной системы** – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

1.41. **Среда функционирования СКЗИ** – совокупность технических и программных средств, совместно с которыми предполагается штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований.

1.42. **Средства криптографической защиты информации (шифровальные (криптографические) средства, криптосредства, СКЗИ) –** средства вычислительной техники, осуществляющие криптографическое преобразование информации для обеспечения ее безопасности.

1.43. **Средство защиты информации** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

1.44. **Средства вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

1.45. **Субъект доступа** – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

1.46. **Технический канал утечки информации** – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

1.47. **Угроза безопасности** – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

1.48. **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.

1.49. **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.

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

1.51. **Уязвимость** – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

1.52. **Характеристика безопасности объекта –** требование к объекту, или к условиям его создания и существования, или к информации об объекте и условиях его создания и существования, выполнение которого необходимо для обеспечения защищенности жизненно важных интересов личности, общества или государства.

1.53. **Целостность информации** – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

1.54. **Электронная подпись –** информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

2. ОСНОВНЫЕ ПОЛОЖЕНИЯ

2.1. В соответствии со статьей 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» в МБДОУ № 44 (далее – Оператор) при обработке ПДн необходимо принимать правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2.2. Мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн включают в себя определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз безопасности ПДн при их обработке в ИСПДн (далее – Модель угроз).

2.3. Передача ПДн осуществляется по телекоммуникационным каналам связи, имеющим выход за пределы контроллируемой зоны (передача данных от клиентской части к серверной).

2.4. К информационным ресурсам ИСПДн осуществляется терминальный доступ, являющегося средством криптографической защиты информации.

2.5. Следовательно, при формировании Модели угроз достаточно использовать методические документы ФСТЭК России.

2.6. Настоящая 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 конкретной ИСПДн;
- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в ИСПДн.

3. ОБЩИЕ ХАРАКТЕРИСТИКИ, СТРУКТУРА И УРОВЕНЬ ИСХОДНОЙ ЗАЩИЩЕННОСТИ ИСПДН

3.1. Состав «ИСПДн МБДОУ № 44»

В Управлении образования используются ИС с использованием технологии удаленного доступа, т.е. элементы ИСПДн разнесены территориально. В ИСПДн связь между территориально удаленными элементами осуществляется по каналам защещенным каналом связи.

АРМ «ИСПДн МБДОУ №44» состоит из пользовательской рабочей станции, которая предоставляет доступ к обработке ПДн в следующих ИС:

- АИС «Электронный детский сад» (модуль «БАРС Образование»);
- ИС «Муниципальный сегмент ГИС РС «Контингент».

3.2. Общие характеристики ИСПДн приведены в Таблице 1.

Таблица 1

№ п/п	Характеристика	Значение характеристики
1.	Состав ИСПДн	-ИСПДн МБДОУ №44
2.	Место нахождения	- г.Ковров ул Моховая д. 2/7
3.	Назначение	АРМ используется сотрудниками для исполнения полномочий, возложенных на Ванюкову Татьяну Николаевну
4.	Территориальное размещение	Распределенная ИСПДн, с доступом к клиентской части, серверная часть не располагается в организации
5.	Наличие соединения с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования
6.	Встроенные (легальные) операции с записями баз персональных данных	Чтение, поиск, запись, удаление, сортировка
7.	Разграничение доступа к персональным данным	ИСПДн, к которой имеют доступ определённые перечнем сотрудники организации
8.	Наличие соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используется база ПДн, которая размещена на серверах, располагающихся не в организации
9.	Уровень обобщения (обезличивания) ПДн	ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)

3.3. Характеристики программных комплексов, входящих в состав ИСПДн МБДОУ №44 приведены в Таблице 2.

Таблица 2

№ п/п	Наименование ПК, входящих в состав ИСПДн	Категории ПДн, обрабатываемых в ПК	Категории субъектов ПДн, обрабатываемых в ПК	Количество субъектов ПДн, обрабатываемых в ПК	Предварительный уровень защищенности ПДн, обрабатываемых в ПК
1.	АИС «Электронная школа», в том числе модуль АИС	Иные	Субъекты, являющиеся сотрудниками	Менее чем 100 000	3УЗ

№ п/п	Наименование ПК, входящих в состав ИСПДн	Категории ПДн, обрабатываемых в ПК	Категории субъектов ПДн, обрабатываемых в ПК	Количество субъектов ПДн, обрабатываемых в ПК	Предварительный уровень защищенности ПДн, обрабатываемых в ПК
	«Питание»		образовательных организаций (далее – ОО), обучающимися ОО, родителями (законными представителями) обучающихся ОО		
2.	АИС «Электронный детский сад»	Иные	Субъекты, являющиеся сотрудниками ОО, воспитанниками ОО, родителями (законными представителями) воспитанников ОО	Менее чем 100 000	3УЗ
3.	АИС «Электронное учреждение дополнительного образования»	Иные	Субъекты, являющиеся сотрудниками ОО, обучающимися ОО, родителями (законными представителями) обучающихся ОО	Менее чем 100 000	3УЗ
4.	АИС «Электронное дистанционное обучение»	Иные	Субъекты, являющиеся сотрудниками ОО, обучающимися ОО	Менее чем 100 000	3УЗ
5.	АИС «Навигатор дополнительного образования»	Иные	Субъекты, являющиеся сотрудниками ОО, обучающимися ОО, родителями (законными представителями) обучающихся ОО	Менее чем 100 000	3УЗ
6.	ИС «Муниципальный сегмент ГИС РС «Контингент»	Иные	Субъекты, являющиеся сотрудниками ОО и УО, обучающимися ОО, родителями (законными представителями) обучающихся ОО	Менее чем 100 000	3УЗ

3.4. Исходя из вышеуказанных характеристик программных комплексов, входящих в состав ИСПДн МБДОУ №44, для ПДн при их обработке в ИСПДн МБДОУ №44 установлен 3 уровень защищенности.

4. КЛАССИФИКАЦИЯ НАРУШИТЕЛЕЙ

4.1. Классификация нарушителей в соответствии с нормативными документами ФСТЭК России.

4.1.1. В соответствии с нормативными документами ФСТЭК России по наличию права постоянного или разового доступа в КЗ ИСПДн нарушители подразделяются на два типа:

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

4.1.2. Границы КЗ ИСПДн определяются Приказом «Об организации контролируемой зоны в МБДОУ №44».

4.1.3. Внешними нарушителями могут быть: конкуренты (конкурирующие организации), недобросовестные партнеры, внешние субъекты (физические лица).

4.1.4. Внешний нарушитель может иметь 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 и (или) сетям международного информационного обмена;
- 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 (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;
- осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн.

4.1.5. Характер и объем ПДн, хранимых и обрабатываемых в ИСПДн, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных на утечку информации по техническим каналам утечки информации. Исходя из этого, в качестве внешнего нарушителя рассматриваются 2 категории лиц:

- физические лица, не являющиеся сотрудниками МБДОУ №44, имеющие возможность осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;

– физические лица, являющиеся сотрудниками МБДОУ №44 и имеющие возможность осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ.

4.1.6. Внутренними нарушителями могут быть:

Кате-гория	Тип внутреннего нарушителя	Возможные нарушители	Предположения
I	Лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн	Обслуживающий персонал МБДОУ №44 (охрана, работники инженерно-технических, административно-хозяйственных служб)	Обслуживающий персонал МБДОУ №44 не имеет доступа в помещения, где расположена ИСПДн, в отсутствие сотрудников МБДОУ №44, поэтому лица категории I исключаются из числа вероятных нарушителей
II	Зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места	Сотрудники МБДОУ №44	Предполагается, что возможности зарегистрированных пользователей, имеющих доступ к ИСПДн, существенным образом не ограничены действующими в пределах контролируемой зоны факторами, поэтому лица категории II не исключаются из числа вероятных нарушителей
III	Зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам		Предполагается, что возможности зарегистрированных пользователей не регламентированы действующими организационно-техническими мерами, направленными на предотвращение и пресечение несанкционированных действий, и существенно не ограничены, поэтому лица категории III не исключаются из числа вероятных нарушителей
IV	Зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн	Ответственный за обеспечение безопасности ПДн в ИСПДн, системные администраторы	К лицам категорий IV, V и VI не применяется комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей. Лица категорий IV, V и VI не исключаются из числа вероятных нарушителей
V	Зарегистрированные пользователи с полномочиями системного администратора ИСПДн		
VI	Зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн		

Кате-гория	Тип внутреннего нарушителя	Возможные нарушители	Предположения
VII	Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте	Разработчики ПО, входящего в состав ИСПДн	Обслуживание программных компонентов ИСПДн осуществляется не доверенными лицами без контроля со стороны ответственного за обеспечение безопасности ПДн в ИСПДн. Поэтому лица категории VII не исключаются из числа вероятных нарушителей

4.1.7. Потенциал нарушителя определяется мерой усилий, затраченных нарушителем при реализации угроз безопасности ПДн, обрабатываемых в ИСПДн.

4.1.8. В зависимости от потенциала, требуемого для реализации угроз безопасности ПДн, обрабатываемых в ИСПДн, нарушители подразделяются на:

- нарушителей, обладающих низким потенциалом (возможности уровня одного человека по приобретению (в свободном доступе на бесплатной или платной основе) и использованию специальных средств эксплуатации уязвимостей).
- нарушителей, обладающих средним потенциалом (возможности уровня группы лиц/организации по разработке и использованию специальных средств эксплуатации уязвимостей).
- нарушителей, обладающих высоким потенциалом (возможности уровня предприятия/группы предприятий/государства по разработке и использованию специальных средств эксплуатации уязвимостей.).

4.1.9. Исходя из целей и задач ИСПДн МБДОУ №44, характера и объема ПДн, хранимых и обрабатываемых в ИСПДн МБДОУ №44, в качестве вероятных нарушителей рассматриваются: внутренний нарушитель со средним потенциалом и внешний нарушитель с низким потенциалом.

5. АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ПДН, ОБРАБАТЫВАЕМЫХ В ИСПДН

5.1. Общие положения

5.1.1. В ИСПДн требуется обеспечить конфиденциальность, защиту от уничтожения и целостность защищаемой информации.

5.1.2. Модель угроз верхнего уровня содержит следующий перечень угроз:

- угроза нарушения конфиденциальности защищаемой информации;
- угроза уничтожения защищаемой информации;
- угроза нарушения целостности защищаемой информации.

5.2. Угрозы безопасности в соответствии с нормативными документами ФСТЭК России

5.2.1. В соответствии с нормативными документами ФСТЭК России возможно возникновение или умышленная реализация следующих групп угроз безопасности ПДн:

- угрозы утечки по техническим каналам;
- угрозы несанкционированного доступа к ПДн.

5.2.2. При обработке ПДн в ИСПДн за счет реализации ТКУИ возможно возникновение следующих угроз безопасности ПДн:

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

5.2.3. Угрозы несанкционированного доступа к ПДн.

5.2.3.1. Угрозы непосредственного доступа к ПДн. Возможные угрозы непосредственного доступа:

- угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;
- угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы, с применением специальных программ для осуществления НСД;
- угрозы внедрения вредоносных программ (локально).

5.2.3.2. Угрозы удаленного доступа. Возможные угрозы удаленного доступа:

- выявление паролей;

– подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа;
– навязывание ложного маршрута сети путем несанкционированного использования протоколов маршрутизации;
– реализация отказа в обслуживании;
– удалённый запуск приложений;
– угрозы внедрения вредоносных программ (по сети).

Угрозы безопасности персональных данных при их передаче по каналам связи КСПД, имеющим выход за пределы КЗ являются неактуальными по причине :

Использование выделенных каналов связи КСПД, предоставляемых на договорной основе ООО «ИТНЕТ». В соответствии с Договором, предоставляемые услуги включают невозможность выхода пакетного трфика за пределы КСПД и проникновение в сеть извне, а также логическое отделение от публичных сетей, для обеспечения защиты передаваемого трафика от несанкционированного доступа извне.

5.3. Анализ возможных угроз

5.3.1. В качестве исходного перечня возможных угроз безопасности ПДн используется банк данных угроз безопасности информации, сформированный ФСТЭК России (http://bdu.fstec.ru/).

5.3.2. Угрозы утечки информации по техническим каналам характеризуются высокой стоимостью оборудования, необходимого для их реализации, и высокой квалификацией нарушителя. Цели и задачи ИСПДн МБДОУ №44 характер и объем ПДн, хранимых и обрабатываемых в ИСПДн, являются недостаточными для мотивации нарушителя к реализации угроз, связанных с техническими каналами утечки информации. Исходя из этого, в данной Модели угроз угрозы утечки информации по техническим каналам утечки информации не рассматриваются.

5.3.3. Перечень возможных угроз безопасности ПДн представлен в Приложении 2.

5.3.4. Анализ возможных угроз безопасности персональных данных приведен в Приложении 3.

5.3.5. По каждому виду угрозы, экспертным путем (опрос специалистов) определены:

– опасность (ущерб) в соответствии со следующими правилами:

Опасность угрозы		
Низкая	**Средняя**	**Высокая**
Реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных	Реализация угрозы может привести к негативным последствиям для субъектов персональных данных	Реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных

– вероятность реализации угрозы (в виде вербальной градации показателя о частоте (вероятности) реализации угрозы безопасности ПДн и соответствующего числового коэффициента Y2) в соответствии со следующими правилами:

Вероятность (Y2)	
Маловероятно	0
Низкая	2
Средняя	5
Высокая	10

5.3.6. Результаты изучения вероятности реализации угроз и опасности угроз приведены в Приложении 4.

5.3.7. С учетом полученных числовых коэффициентов Y1 и Y2 по каждому виду угрозы безопасности ПДн рассчитан числовой коэффициент реализуемости угрозы Y и определена вербальная интерпретация реализуемости конкретной угрозы безопасности ПДн в соответствии с формулами:

$$Y = (Y1+Y2)/20$$

Значение числового коэффициента реализуемости угрозы Y	**Возможность реализации угрозы**
$0 \leq Y \leq 0,3$	Низкая
$0,3 < Y \leq 0,6$	Средняя
$0,6 < Y \leq 0,8$	Высокая
$Y > 0,8$	Очень высокая

5.3.8. При определении степени опасности угроз утечки информации по техническим каналам связи учитывались границы контролируемой зоны (КЗ) и размещение технических средств.

5.3.9. Определена актуальность угроз безопасности ПДн на основании коэффициента реализуемости угрозы (Y) и показателя опасности угрозы по каждому ее виду, сделан вывод об актуальности угроз в соответствии со следующими правилами:

Возможность реализации угрозы	**Опасность угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная
Очень высокая	Актуальная	Актуальная	Актуальная

6. ВЫВОДЫ

6.1. Актуальные угрозы

6.1.1. В результате анализа возможных угроз безопасности персональных данных выявлено актуальных угроз безопасности: 74.

№ п/п	Угроза	Тип угроз
1.	Угроза внедрения кода или данных	Угрозы 3-го типа
2.	Угроза воздействия на программы с высокими привилегиями	Угрозы 3-го типа
3.	Угроза восстановления аутентификационной информации	Угрозы 3-го типа
4.	Угроза доступа к защищаемым файлам с использованием обходного пути	Угрозы 3-го типа
5.	Угроза заражения DNS-кеша	Угрозы 3-го типа
6.	Угроза избыточного выделения оперативной памяти	Угрозы 3-го типа
7.	Угроза изменения системных и глобальных переменных	Угрозы 3-го типа
8.	Угроза искажения XML-схемы	Угрозы 3-го типа
9.	Угроза использования альтернативных путей доступа к ресурсам	Угрозы 3-го типа
10.	Угроза использования механизмов авторизации для повышения привилегий	Угрозы 3-го типа
11.	Угроза использования слабостей протоколов сетевого/локального обмена данными	Угрозы 3-го типа
12.	Угроза исследования механизмов работы программы	Угрозы 3-го типа
13.	Угроза исследования приложения через отчёты об ошибках	Угрозы 3-го типа
14.	Угроза межсайтового скриптинга	Угрозы 3-го типа
15.	Угроза нарушения целостности данных кеша	Угрозы 3-го типа
16.	Угроза некорректного задания структуры данных транзакции	Угрозы 3-го типа
17.	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Угрозы 3-го типа
18.	Угроза некорректного использования функционала программного обеспечения	Угрозы 3-го типа
19.	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Угрозы 3-го типа
20.	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Угрозы 3-го типа
21.	Угроза несанкционированного доступа к аутентификационной информации	Угрозы 3-го типа
22.	Угроза несанкционированного изменения аутентификационной информации	Угрозы 3-го типа
23.	Угроза несанкционированного копирования защищаемой информации	Угрозы 3-го типа
24.	Угроза несанкционированного редактирования реестра	Угрозы 3-го типа
25.	Угроза несанкционированного создания учётной записи пользователя	Угрозы 3-го типа
26.	Угроза несанкционированного удаления защищаемой информации	Угрозы 3-го типа
27.	Угроза несанкционированного управления буфером	Угрозы 3-го типа
28.	Угроза несанкционированного управления синхронизацией и состоянием	Угрозы 3-го типа
29.	Угроза несанкционированного управления указателями	Угрозы 3-го типа
30.	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Угрозы 3-го типа
31.	Угроза обнаружения хостов	Угрозы 3-го типа

№ п/п	Угроза	Тип угроз
32.	Угроза обхода некорректно настроенных механизмов аутентификации	Угрозы 3-го типа
33.	Угроза опосредованного управления группой программ через совместно используемые данные	Угрозы 3-го типа
34.	Угроза определения типов объектов защиты	Угрозы 3-го типа
35.	Угроза определения топологии вычислительной сети	Угрозы 3-го типа
36.	Угроза перебора всех настроек и параметров приложения	Угрозы 3-го типа
37.	Угроза передачи данных по скрытым каналам	Угрозы 3-го типа
38.	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Угрозы 3-го типа
39.	Угроза перехвата данных, передаваемых по вычислительной сети	Угрозы 3-го типа
40.	Угроза перехвата привилегированного потока	Угрозы 3-го типа
41.	Угроза перехвата привилегированного процесса	Угрозы 3-го типа
42.	Угроза повреждения системного реестра	Угрозы 3-го типа
43.	Угроза повышения привилегий	Угрозы 3-го типа
44.	Угроза подделки записей журнала регистрации событий	Угрозы 3-го типа
45.	Угроза подмены доверенного пользователя	Угрозы 3-го типа
46.	Угроза подмены содержимого сетевых ресурсов	Угрозы 3-го типа
47.	Угроза приведения системы в состояние «отказ в обслуживании»	Угрозы 3-го типа
48.	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Угрозы 3-го типа
49.	Угроза пропуска проверки целостности программного обеспечения	Угрозы 3-го типа
50.	Угроза сбоя обработки специальным образом изменённых файлов	Угрозы 3-го типа
51.	Угроза сбоя процесса обновления BIOS	Угрозы 3-го типа
52.	Угроза удаления аутентификационной информации	Угрозы 3-го типа
53.	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Угрозы 3-го типа
54.	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Угрозы 3-го типа
55.	Угроза утраты вычислительных ресурсов	Угрозы 3-го типа
56.	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Угрозы 3-го типа
57.	Угроза форматирования носителей информации	Угрозы 3-го типа
58.	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Угрозы 3-го типа
59.	Угроза эксплуатации цифровой подписи программного кода	Угрозы 3-го типа
60.	Угроза перехвата исключения/сигнала из привилегированного блока функций	Угрозы 3-го типа
61.	Угроза включения в проект не достоверно испытанных компонентов	Угрозы 3-го типа
62.	Угроза внедрения системной избыточности	Угрозы 3-го типа
63.	Угроза наличия механизмов разработчика	Угрозы 3-го типа
64.	Угроза неправомерного шифрования информации	Угрозы 3-го типа
65.	Угроза скрытного включения вычислительного устройства в состав бот-сети	Угрозы 3-го типа
66.	Угроза распространения «почтовых червей»	Угрозы 3-го типа
67.	Угроза «фарминга»	Угрозы 3-го типа
68.	Угроза «фишинга»	Угрозы 3-го типа
69.	Угроза несанкционированного использования системных и сетевых утилит	Угрозы 3-го типа
70.	Угроза несанкционированной модификации защищаемой информации	Угрозы 3-го типа
71.	Угроза подмены программного обеспечения	Угрозы 3-го типа

№ п/п	Угроза	Тип угроз
72.	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Угрозы 3-го типа
73.	Угроза использования уязвимых версий программного обеспечения	Угрозы 3-го типа
74.	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Угрозы 3-го типа

6.1.2. Выявленные актуальные угрозы безопасности ПДн в ИСПДн относятся к угрозам 3-го типа: угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Приложение 1. Анализ уточненных возможностей нарушителей и направления атак

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
1.	Проведение атаки при нахождении в пределах контролируемой зоны	Актуально	Объективные предпосылки для реализации угрозы существуют: – в помещениях, в которых происходит обработка ПДн, возможно нахождение посторонних лиц; – ремонт, обслуживание и сопровождение программных, технических и программно-технических средств ИСПДн, в том числе СЗИ, выполняется не доверенными лицами, без выполнения мер по обеспечению безопасности ПДн; – не используются сертифицированные средства антивирусной защиты; – не используются сертифицированные средства защиты информации от несанкционированного доступа; но приняты меры по обеспечению безопасности ПДн: – обслуживающий персонал и лица, обеспечивающие функционирование ИСПДн, не имеют возможности находиться в помещениях, где расположена ИСПДн, в отсутствие пользователей ИСПДн; – работа пользователей ИСПДн регламентирована должностными инструкциями; – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – Проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы;
2.	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	Не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности

Приложение 2. Перечень возможных угроз безопасности ПДн

Идентификатор угрозы	Наименование угрозы	Деструктивное воздействие на информацию
УБИ.001	Угроза автоматического распространения вредоносного кода в грид-системе	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.006	Угроза внедрения кода или данных	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.007	Угроза воздействия на программы с высокими привилегиями	Нарушение конфиденциальности, нарушение целостности
УБИ.008	Угроза восстановления аутентификационной информации	Нарушение конфиденциальности
УБИ.010	Угроза выхода процесса за пределы виртуальной машины	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.011	Угроза деавторизации санкционированного клиента беспроводной сети	Нарушение доступности
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	Нарушение доступности
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	Нарушение конфиденциальности
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies	Нарушение конфиденциальности, нарушение доступности
УБИ.019	Угроза заражения DNS-кеша	Нарушение конфиденциальности
УБИ.021	Угроза злоупотребления доверием потребителей облачных услуг	Нарушение конфиденциальности, нарушение целостности
УБИ.022	Угроза избыточного выделения оперативной памяти	Нарушение доступности
УБИ.025	Угроза изменения системных и глобальных переменных	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.026	Угроза искажения XML-схемы	Нарушение целостности, нарушение доступности
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	Нарушение конфиденциальности
УБИ.029	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	Нарушение доступности
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	Нарушение конфиденциальности

Идентификатор угрозы	Наименование угрозы	Деструктивное воздействие на информацию
УБИ.033	Угроза использования слабостей кодирования входных данных	Нарушение целостности, нарушение доступности
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Нарушение конфиденциальности
УБИ.036	Угроза исследования механизмов работы программы	Нарушение конфиденциальности, нарушение доступности
УБИ.037	Угроза исследования приложения через отчёты об ошибках	Нарушение конфиденциальности
УБИ.040	Угроза конфликта юрисдикций различных стран	Нарушение доступности
УБИ.041	Угроза межсайтового скриптинга	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.043	Угроза нарушения доступности облачного сервера	Нарушение доступности
УБИ.044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Нарушение конфиденциальности, нарушение доступности
УБИ.047	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Нарушение доступности
УБИ.048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.049	Угроза нарушения целостности данных кеша	Нарушение целостности, нарушение доступности
УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Нарушение целостности, нарушение доступности
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.055	Угроза незащищённого администрирования облачных услуг	Нарушение конфиденциальности, нарушение целостности, нарушение доступности

Идентификатор угрозы	Наименование угрозы	Деструктивное воздействие на информацию
УБИ.056	Угроза некачественного переноса инфраструктуры в облако	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.058	Угроза неконтролируемого роста числа виртуальных машин	Нарушение доступности
УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Нарушение доступности
УБИ.061	Угроза некорректного задания структуры данных транзакции	Нарушение целостности, нарушение доступности
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Нарушение конфиденциальности
УБИ.063	Угроза некорректного использования функционала программного и аппаратного обеспечения	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.064	Угроза некорректной реализации политики лицензирования в облаке	Нарушение доступности
УБИ.065	Угроза неопределённости в распределении ответственности между ролями в облаке	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.066	Угроза неопределённости ответственности за обеспечение безопасности облака	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.069	Угроза неправомерных действий в каналах связи	Нарушение конфиденциальности, нарушение целостности
УБИ.070	Угроза непрерывной модернизации облачной инфраструктуры	Нарушение целостности, нарушение доступности
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации	Нарушение конфиденциальности
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Нарушение конфиденциальности

Идентификатор угрозы	Наименование угрозы	Деструктивное воздействие на информацию
УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи	Нарушение конфиденциальности
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Нарушение доступности
УБИ.077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	Нарушение целостности, нарушение доступности
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.082	Угроза несанкционированного доступа к сегментам вычислительного поля	Нарушение конфиденциальности, нарушение целостности
УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Нарушение конфиденциальности
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Нарушение целостности, нарушение доступности
УБИ.088	Угроза несанкционированного копирования защищаемой информации	Нарушение конфиденциальности
УБИ.089	Угроза несанкционированного редактирования реестра	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.091	Угроза несанкционированного удаления защищаемой информации	Нарушение доступности

Идентификатор угрозы	Наименование угрозы	Деструктивное воздействие на информацию
УБИ.093	Угроза несанкционированного управления буфером	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием	Нарушение целостности, нарушение доступности
УБИ.095	Угроза несанкционированного управления указателями	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	Нарушение конфиденциальности
УБИ.099	Угроза обнаружения хостов	Нарушение конфиденциальности
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные	Нарушение целостности, нарушение доступности
УБИ.103	Угроза определения типов объектов защиты	Нарушение конфиденциальности
УБИ.104	Угроза определения топологии вычислительной сети	Нарушение конфиденциальности
УБИ.109	Угроза перебора всех настроек и параметров приложения	Нарушение целостности, нарушение доступности
УБИ.111	Угроза передачи данных по скрытым каналам	Нарушение конфиденциальности
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Нарушение целостности, нарушение доступности
УБИ.114	Угроза переполнения целочисленных переменных	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Нарушение конфиденциальности
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	Нарушение конфиденциальности

Идентификатор угрозы	Наименование угрозы	Деструктивное воздействие на информацию
УБИ.117	Угроза перехвата привилегированного потока	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.118	Угроза перехвата привилегированного процесса	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.119	Угроза перехвата управления гипервизором	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.120	Угроза перехвата управления средой виртуализации	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.121	Угроза повреждения системного реестра	Нарушение целостности, нарушение доступности
УБИ.122	Угроза повышения привилегий	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.124	Угроза подделки записей журнала регистрации событий	Нарушение целостности
УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.126	Угроза подмены беспроводного клиента или точки доступа	Нарушение конфиденциальности, нарушение доступности
УБИ.128	Угроза подмены доверенного пользователя	Нарушение конфиденциальности
УБИ.130	Угроза подмены содержимого сетевых ресурсов	Нарушение конфиденциальности
УБИ.133	Угроза получения сведений о владельце беспроводного устройства	Нарушение конфиденциальности
УБИ.134	Угроза потери доверия к поставщику облачных услуг	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	Нарушение доступности
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Нарушение целостности, нарушение доступности

Идентификатор угрозы	Наименование угрозы	Деструктивное воздействие на информацию
УБИ.145	Угроза пропуска проверки целостности программного обеспечения	Нарушение целостности, нарушение доступности
УБИ.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Нарушение конфиденциальности
УБИ.147	Угроза распространения несанкционированно повышенных прав на всю грид-систему	Нарушение конфиденциальности, нарушение целостности
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.150	Угроза сбоя процесса обновления BIOS	Нарушение доступности
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Нарушение конфиденциальности
УБИ.152	Угроза удаления аутентификационной информации	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Нарушение доступности
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.155	Угроза утраты вычислительных ресурсов	Нарушение доступности
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Нарушение целостности, нарушение доступности
УБИ.158	Угроза форматирования носителей информации	Нарушение целостности, нарушение доступности
УБИ.159	Угроза «форсированного веб-браузинга»	Нарушение конфиденциальности
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Нарушение конфиденциальности, нарушение доступности
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Нарушение конфиденциальности, нарушение целостности, нарушение доступности

Идентификатор угрозы	Наименование угрозы	Деструктивное воздействие на информацию
УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.166	Угроза внедрения системной избыточности	Нарушение доступности
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Нарушение конфиденциальности, нарушение доступности
УБИ.169	Угроза наличия механизмов разработчика	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.170	Угроза неправомерного шифрования информации	Нарушение доступности
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	Нарушение доступности
УБИ.172	Угроза распространения «почтовых червей»	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.173	Угроза «спама» веб-сервера	Нарушение доступности
УБИ.174	Угроза «фарминга»	Нарушение конфиденциальности
УБИ.175	Угроза «фишинга»	Нарушение конфиденциальности
УБИ.176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты	Нарушение доступности
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.179	Угроза несанкционированной модификации защищаемой информации	Нарушение целостности
УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Нарушение целостности, нарушение доступности
УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Нарушение конфиденциальности

Идентификатор угрозы	Наименование угрозы	Деструктивное воздействие на информацию
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.188	Угроза подмены программного обеспечения	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.192	Угроза использования уязвимых версий программного обеспечения	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Нарушение конфиденциальности
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Нарушение доступности
УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Нарушение доступности
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Нарушение конфиденциальности, нарушение целостности, нарушение доступности
УБИ.212	Угроза перехвата управления информационной системой	Нарушение конфиденциальности, нарушение целостности, нарушение доступности

Приложение 3. Вербальная оценка вероятности угроз в ИСПДн МБДОУ №44

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	**Вероятность**	**Комментарий**
УБИ.001	Угроза автоматического распространения вредоносного кода в грид-системе	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии грид-систем.
УБИ.006	Угроза внедрения кода или данных	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют, но приняты меры по обеспечению безопасности ПДн: – пользователи ИСПДн не имеют возможности запуска стороннего или установки, изменения настроек имеющегося программного обеспечения без контроля со стороны ответственного за обеспечение безопасности ПДн; – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы.
УБИ.007	Угроза воздействия на программы с высокими привилегиями	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют, но приняты меры по обеспечению безопасности ПДн: – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – работа пользователей ИСПДн регламентирована должностными инструкциями; – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ.008	Угроза восстановления аутентификационной информации	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют, но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ.010	Угроза выхода процесса за пределы виртуальной машины	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии виртуализации.
УБИ.011	Угроза деавторизации санкционированного клиента беспроводной сети	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии беспроводного доступа.
УБИ.014	Угроза длительного удержания вычислительных	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы:

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
	ресурсов пользователями			– программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства, в том числе и СЗИ, настроены доверенными лицами и соответствуют требованиям по защите ПДн; – работа пользователей ИСПДн регламентирована должностными инструкциями.
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются веб-серверы.
УБИ.019	Угроза заражения DNS-кеша	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют, но приняты меры по обеспечению безопасности ПДн: – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы.
УБИ.021	Угроза злоупотребления доверием потребителей облачных услуг	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – оператор не является потребителем облачных услуг.
УБИ.022	Угроза избыточного выделения оперативной памяти	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют, но приняты меры по обеспечению безопасности ПДн: – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы.
УБИ.025	Угроза изменения системных и глобальных переменных	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы.
УБИ.026	Угроза искажения XML-схемы	Низкая	Высокая	Отсутствуют объективные предпосылки для осуществления угрозы: – не осуществляется удаленный доступ сотрудников организации к информационным ресурсам ИСПДн;

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
				– действующие требования по обеспечению безопасности ПДн не предусматривают обязательное использование СКЗИ. ИСПДн функционирует с использованием выделенных каналов связи, предоставляемых ООО «ИТНЕТ», что исключает возможность выхода трафика за переделы КСПД, проникновение в сеть извне, а также осуществляет логическое отделение от публичных сетей.
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	Низкая	Высокая	Отсутствуют объективные предпосылки для осуществления угрозы: – действующие требования по обеспечению безопасности ПДн не предусматривают обязательное использование СКЗИ. ИСПДн функционирует с использованием выделенных каналов связи, предоставляемых ООО «ИТНЕТ», что исключает возможность выхода трафика за переделы КСПД, проникновение в сеть извне, а также осуществляет логическое отделение от публичных; – Подготовка для просмотра информации происходит на кластере серверов.
УБИ.029	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии суперкомпьютерных систем.
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	Средняя	Средняя	Отсутствуют объективные предпосылки для осуществления угрозы: – действующие требования по обеспечению безопасности ПДн не предусматривают обязательное использование СКЗИ. ИСПДн функционирует с использованием выделенных каналов связи, предоставляемых ООО «ИТНЕТ», что исключает возможность выхода трафика за переделы КСПД, проникновение в сеть извне, а также осуществляет логическое отделение от публичных; – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ.033	Угроза использования слабостей кодирования входных данных	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют, но приняты меры по обеспечению безопасности ПДн: – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – действующие требования по обеспечению безопасности ПДн не предусматривают обязательное использование СКЗИ. ИСПДн функционирует с использованием выделенных каналов связи, предоставляемых ООО «ИТНЕТ», что исключает возможность выхода трафика за переделы КСПД, проникновение в сеть извне, а также осуществляет логическое отделение от публичных сетей в ИСПДн не используются сертифицированные средства межсетевого экранирования; – не осуществляется удаленный доступ сотрудников организации к информационным ресурсам ИСПДн.
УБИ.036	Угроза исследования механизмов работы программы	Низкая	Маловероятно	– Отсутствуют объективные предпосылки для осуществления угрозы
УБИ.037	Угроза исследования приложения через отчёты об ошибках	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ.040	Угроза конфликта юрисдикций различных стран	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – трансграничная передача ПДн не осуществляется.
УБИ.041	Угроза межсайтового скриптинга	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства межсетевого экранирования; Но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн; – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы.

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
УБИ.043	Угроза нарушения доступности облачного сервера	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – оператор не является поставщиком облачных услуг; – оператор не является потребителем облачных услуг.
УБИ.044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии виртуализации.
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ.047	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии грид-систем.
УБИ.048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии виртуализации; – оператор не является потребителем облачных услу.
УБИ.049	Угроза нарушения целостности данных кеша	Низкая	Высокая	Отсутствуют объективные предпосылки для осуществления угрозы: – действующие требования по обеспечению безопасности ПДн не предусматривают обязательное использование СКЗИ. ИСПДн функционирует с использованием выделенных каналов связи, предоставляемых ООО «ИТНЕТ», что исключает возможность выхода трафика за переделы КСПД, проникновение в сеть извне, а также осуществляет логическое отделение от публичных .
УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – оператор не является потребителем облачных услуг.
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – оператор не является потребителем облачных услуг
УБИ.055	Угроза незащищённого администрирования облачных услуг	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – оператор не является потребителем облачных услуг.
УБИ.056	Угроза некачественного переноса инфраструктуры в облако	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – оператор ИСПДн не заинтересован в переносе инфраструктуры ИСПДн в облако.
УБИ.058	Угроза неконтролируемого роста числа виртуальных машин	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии виртуализации; – оператор не является потребителем облачных услуг.

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии виртуализации.
УБИ.061	Угроза некорректного задания структуры данных транзакции	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют, но приняты меры по обеспечению безопасности ПДн: – работа пользователей ИСПДн регламентирована должностными инструкциями.
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Средняя	Средняя	Отсутствуют объективные предпосылки для осуществления угрозы: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн; – действующие требования по обеспечению безопасности ПДн не предусматривают обязательное использование СКЗИ. ИСПДн функционирует с использованием выделенных каналов связи, предоставляемых ООО «ИТНЕТ», что исключает возможность выхода трафика за переделы КСПД, проникновение в сеть извне, а также осуществляет логическое отделение от публичных; – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение.
УБИ.063	Угроза некорректного использования функционала программного обеспечения	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют, но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн; – работа пользователей ИСПДн регламентирована должностными инструкциями.
УБИ.064	Угроза некорректной реализации политики лицензирования в облаке	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – оператор не является потребителем облачных услуг; – оператор не является поставщиком облачных услуг.
УБИ.065	Угроза неопределённости в распределении ответственности между ролями в облаке	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – оператор не является потребителем облачных услуг; – оператор не является поставщиком облачных услуг.
УБИ.066	Угроза неопределённости ответственности за обеспечение безопасности облака	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – оператор не является потребителем облачных услуг; – оператор не является поставщиком облачных услуг.

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ.069	Угроза неправомерных действий в каналах связи	Низкая	Высокая	Отсутствуют объективные предпосылки для осуществления угрозы: – не осуществляется удаленный доступ сотрудников организации к информационным ресурсам ИСПДн; – действующие требования по обеспечению безопасности ПДн не предусматривают обязательное использование СКЗИ. ИСПДн функционирует с использованием выделенных каналов связи, предоставляемых ООО «ИТНЕТ», что исключает возможность выхода трафика за переделы КСПД, проникновение в сеть извне, а также осуществляет логическое отделение от публичных сетей.
УБИ.070	Угроза непрерывной модернизации облачной инфраструктуры	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – оператор не является поставщиком облачных услуг; – оператор не является потребителем облачных услуг.
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации	Низкая	Высокая	Отсутствуют объективные предпосылки для осуществления угрозы: – доступ к ИСПДн осуществляется в терминальном режиме, все файлы хранятся на кластере серверов.
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства межсетевого экранирования;
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа.
УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии виртуализации.
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии виртуализации.
УБИ.077	Угроза несанкционированного доступа к	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы:

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
	данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение			– в ИСПДн не используются технологии виртуализации.
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии виртуализации.
УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии виртуализации.
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии виртуализации.
УБИ.082	Угроза несанкционированного доступа к сегментам вычислительного поля	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии суперкомпьютерных систем.
УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии беспроводного доступа.
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии виртуализации.
УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии виртуализации.
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа.
УБИ.088	Угроза несанкционированного копирования защищаемой информации	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в помещениях, в которых происходит обработка ПДн, возможно нахождение посторонних лиц; – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – обслуживающий персонал и лица, обеспечивающие функционирование ИСПДн, не имеют возможности

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
				находиться в помещениях, где расположена ИСПДн, в отсутствие пользователей ИСПДн; – работа пользователей ИСПДн регламентирована должностными инструкциями.
УБИ.089	Угроза несанкционированного редактирования реестра	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ.091	Угроза несанкционированного удаления защищаемой информации	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в помещениях, в которых происходит обработка ПДн, возможно нахождение посторонних лиц; – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – обслуживающий персонал и лица, обеспечивающие функционирование ИСПДн, не имеют возможности находиться в помещениях, где расположена ИСПДн, в отсутствие пользователей ИСПДн; – работа пользователей ИСПДн регламентирована должностными инструкциями; – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение.
УБИ.093	Угроза несанкционированного управления буфером	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа;

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
				Но приняты меры по обеспечению безопасности ПДн: – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы.
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа; Но приняты меры по обеспечению безопасности ПДн: – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы.
УБИ.095	Угроза несанкционированного управления указателями	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа; Но приняты меры по обеспечению безопасности ПДн: – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы.
УБИ.096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – оператор не является потребителем облачных услуг
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства межсетевого экранирования.
УБИ.099	Угроза обнаружения хостов	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства межсетевого экранирования.
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа; Но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
				средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ.103	Угроза определения типов объектов защиты	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства межсетевого экранирования.
УБИ.104	Угроза определения топологии вычислительной сети	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства межсетевого экранирования.
УБИ.109	Угроза перебора всех настроек и параметров приложения	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют, но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн; – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение.
УБИ.111	Угроза передачи данных по скрытым каналам	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – работа пользователей ИСПДн регламентирована должностными инструкциями; – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение.
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Средняя	Средняя	Отсутствуют объективные предпосылки для осуществления угрозы: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн; – работа пользователей ИСПДн регламентирована должностными инструкциями; – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение.
УБИ.114	Угроза переполнения целочисленных переменных	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – программные, технические, программно-технические

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
				средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют, но приняты меры по обеспечению безопасности ПДн: – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы.
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют, но приняты меры по обеспечению безопасности ПДн: – не осуществляется удаленный доступ сотрудников организации к информационным ресурсам ИСПДн; – действующие требования по обеспечению безопасности ПДн не предусматривают обязательное использование СКЗИ. ИСПДн функционирует с использованием выделенных каналов связи, предоставляемых ООО «ИТНЕТ», что исключает возможность выхода трафика за переделы КСПД, проникновение в сеть извне, а также осуществляет логическое отделение от публичных сетей.
УБИ.117	Угроза перехвата привилегированного потока	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа.
УБИ.118	Угроза перехвата привилегированного процесса	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа.
УБИ.119	Угроза перехвата управления гипервизором	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии виртуализации.
УБИ.120	Угроза перехвата управления средой виртуализации	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии виртуализации.
УБИ.121	Угроза повреждения системного реестра	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ.122	Угроза повышения привилегий	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
				защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ.124	Угроза подделки записей журнала регистрации событий	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии беспроводного доступа.
УБИ.126	Угроза подмены беспроводного клиента или точки доступа	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии беспроводного доступа.
УБИ.128	Угроза подмены доверенного пользователя	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства межсетевого экранирования.
УБИ.130	Угроза подмены содержимого сетевых ресурсов	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства межсетевого экранирования; – в ИСПДн не используются сертифицированные СКЗИ. Но приняты меры по обеспечению безопасности ПДн: – действующие требования по обеспечению безопасности ПДн не предусматривают обязательное использование СКЗИ. ИСПДн функционирует с использованием выделенных каналов связи, предоставляемых ООО «ИТНЕТ», что исключает возможность выхода трафика за переделы КСПД, проникновение в сеть извне, а также осуществляет логическое отделение от публичных сетей.
УБИ.133	Угроза получения сведений о владельце беспроводного устройства	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии беспроводного доступа.

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
УБИ.134	Угроза потери доверия к поставщику облачных услуг	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – оператор не является потребителем облачных услуг.
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – оператор ИСПДн не заинтересован в переносе инфраструктуры ИСПДн в облако.
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	Низкая	Высокая	Объективные предпосылки для осуществления угроз существуют: – в ИСПДн не используются сертифицированные средства межсетевого экранирования.
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ.145	Угроза пропуска проверки целостности программного обеспечения	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа; – в ИСПДн не используются сертифицированные средства межсетевого экранирования; Но приняты меры по обеспечению безопасности ПДн: – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы; – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение.
УБИ.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии суперкомпьютерных систем.
УБИ.147	Угроза распространения несанкционированно повышенных прав на всю грид-систему	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются технологии грид-систем систем.
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа.
УБИ.150	Угроза сбоя процесса обновления BIOS	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют
УБИ.151	Угроза сканирования веб-сервисов,	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы:

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
	разработанных на основе языка описания WSDL			– в ИСПДн не используются веб-серверы.
УБИ.152	Угроза удаления аутентификационной информации	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства межсетевого экранирования.
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют
УБИ.155	Угроза утраты вычислительных ресурсов	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства межсетевого экранирования. Но приняты меры по обеспечению безопасности ПДн: – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы.
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в помещениях, в которых происходит обработка ПДн, возможно нахождение посторонних лиц; Но приняты меры по обеспечению безопасности ПДн: – обслуживающий персонал и лица, обеспечивающие функционирование ИСПДн, не имеют возможности находиться в помещениях, где расположена ИСПДн, в отсутствие пользователей ИСПДн; – работа пользователей ИСПДн регламентирована должностными инструкциями.
УБИ.158	Угроза форматирования носителей информации	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
УБИ.159	Угроза «форсированного веб-браузинга»	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются веб-серверы.
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в помещениях, в которых происходит обработка ПДн, возможно нахождение посторонних лиц; Но приняты меры по обеспечению безопасности ПДн: – обслуживающий персонал и лица, обеспечивающие функционирование ИСПДн, не имеют возможности находиться в помещениях, где расположена ИСПДн, в отсутствие пользователей ИСПДн; – работа пользователей ИСПДн регламентирована должностными инструкциями.
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – пользователи ИСПДн не имеют возможности запуска стороннего или установки, изменения настроек имеющегося программного обеспечения без контроля со стороны ответственного за обеспечение безопасности ПДн.
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа.
УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – оператор не является поставщиком облачных услуг.
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют
УБИ.166	Угроза внедрения системной избыточности	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют, но приняты меры по обеспечению безопасности ПДн: – пользователи ИСПДн не имеют возможности запуска стороннего или установки, изменения настроек имеющегося программного обеспечения без контроля со стороны ответственного за обеспечение безопасности ПДн.
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются веб-серверы.
УБИ.169	Угроза наличия механизмов разработчика	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют,

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
				но приняты меры по обеспечению безопасности ПДн: – работа пользователей ИСПДн регламентирована должностными инструкциями.
УБИ.170	Угроза неправомерного шифрования информации	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – работа пользователей ИСПДн регламентирована должностными инструкциями; – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы.
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства межсетевого экранирования. Но приняты меры по обеспечению безопасности ПДн: – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы.
УБИ.172	Угроза распространения «почтовых червей»	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства антивирусной защиты. Но приняты меры по обеспечению безопасности ПДн: – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы.
УБИ.173	Угроза «спама» веб-сервера	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются веб-серверы.
УБИ.174	Угроза «фарминга»	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства межсетевого экранирования. Но приняты меры по обеспечению безопасности ПДн: – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы; – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
				ответственности за их несоблюдение.
УБИ.175	Угроза «фишинга»	Низкая	Высокая	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства межсетевого экранирования. Но приняты меры по обеспечению безопасности ПДн: – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы; – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение.
УБИ.176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – используемые средства защиты информации не накладывают существенных временны́х задержек на процесс обработки ПДн.
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства, в том числе и СЗИ, настроены доверенными лицами и соответствуют требованиям по защите ПДн; – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – работа пользователей ИСПДн регламентирована должностными инструкциями.
УБИ.179	Угроза несанкционированной модификации защищаемой информации	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют: – в помещениях, в которых происходит обработка ПДн, возможно нахождение посторонних лиц; – в ИСПДн не используются сертифицированные средства защиты информации от несанкционированного доступа. Но приняты меры по обеспечению безопасности ПДн: – обслуживающий персонал и лица, обеспечивающие функционирование ИСПДн, не имеют возможности находиться в помещениях, где расположена ИСПДн, в отсутствие пользователей ИСПДн;

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
				– работа пользователей ИСПДн регламентирована должностными инструкциями.
УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – автоматизированные системы управления технологическими процессами в ИСПДн не используются.
УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются мобильные технические средства.
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются средства защиты информации.
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются средства защиты информации.
УБИ.188	Угроза подмены программного обеспечения	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют, но приняты меры по обеспечению безопасности ПДн: – пользователи ИСПДн не имеют возможности запуска стороннего или установки, изменения настроек имеющегося программного обеспечения без контроля со стороны ответственного за обеспечение безопасности ПДн; – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы; – работа пользователей ИСПДн регламентирована должностными инструкциями.
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Средняя	Средняя	Объективные предпосылки для осуществления угрозы существуют, но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн; – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы; – работа пользователей ИСПДн регламентирована должностными инструкциями – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение.
УБИ.192	Угроза использования уязвимых версий	Средняя	Средняя	Отсутствуют объективные предпосылки для осуществления угрозы:

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
	программного обеспечения			– работа пользователей ИСПДн регламентирована должностными инструкциями; – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн; – в ИСПДн осуществляется контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Средняя	Маловероятно	Потенциал возможного нарушителя является недостаточным для осуществления данной угрозы
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Низкая	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – в ИСПДн не используются средства защиты информации;
УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	Низкая	Маловероятно	Объективные предпосылки для осуществления угрозы существуют: – ремонт, обслуживание и сопровождение программных, технических и программно-технических средств ИСПДн выполняется не доверенными лицами, без выполнения мер по обеспечению безопасности ПДн. Но приняты меры по обеспечению безопасности ПДн: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн.
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Средняя	Низкая	Объективные предпосылки для осуществления угрозы существуют: – в помещениях, в которых происходит обработка ПДн, возможно нахождение посторонних лиц; Но приняты меры по обеспечению безопасности ПДн: – проводится регулярное обновление баз вирусных сигнатур, а также проверки ПК на действующие вирусные угрозы; – проводится обучение пользователей ИСПДн мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – пользователи ИСПДн не имеют возможности запуска

Идентификатор угрозы	Наименование угрозы	Вербальная оценка		
		Опасность	Вероятность	Комментарий
				стороннего или установки, изменения настроек имеющегося программного обеспечения без контроля со стороны ответственного за обеспечение безопасности ПДн.
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Средняя	Маловероятно	Потенциал возможного нарушителя является недостаточным для осуществления данной угрозы
УБИ.212	Угроза перехвата управления информационной системой	Средняя	Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы: – программные, технические, программно-технические средства настроены доверенными лицами и соответствуют требованиям по защите ПДн; – доступ к ИСПДн осуществляется в терминальном режиме, централизованное управление осуществляется на кластере серверов Генеральной дирекции.

Приложение 4. Определение актуальности угроз в ИСПДн МБДОУ №44

Идентификатор угрозы	Наименование угрозы	Y2	Y	Реализуемость	Актуальность
УБИ.001	Угроза автоматического распространения вредоносного кода в грид-системе	0	0.25	Низкая	Неактуальная
УБИ.006	Угроза внедрения кода или данных	5	0.5	Средняя	Актуальная
УБИ.007	Угроза воздействия на программы с высокими привилегиями	5	0.5	Средняя	Актуальная
УБИ.008	Угроза восстановления аутентификационной информации	5	0.5	Средняя	Актуальная
УБИ.010	Угроза выхода процесса за пределы виртуальной машины	0	0.25	Низкая	Неактуальная
УБИ.011	Угроза деавторизации санкционированного клиента беспроводной сети	0	0.25	Низкая	Неактуальная
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	0	0.25	Низкая	Неактуальная
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	5	0.5	Средняя	Актуальная
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies	0	0.25	Низкая	Неактуальная
УБИ.019	Угроза заражения DNS-кеша	10	0.75	Высокая	Актуальная
УБИ.021	Угроза злоупотребления доверием потребителей облачных услуг	0	0.25	Низкая	Неактуальная
УБИ.022	Угроза избыточного выделения оперативной памяти	10	0.75	Высокая	Актуальная
УБИ.025	Угроза изменения системных и глобальных переменных	10	0.75	Высокая	Актуальная
УБИ.026	Угроза искажения XML-схемы	10	0.75	Высокая	Актуальная
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	10	0.75	Высокая	Актуальная
УБИ.029	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	0	0.25	Низкая	Неактуальная
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	5	0.5	Средняя	Актуальная
УБИ.033	Угроза использования слабостей кодирования входных данных	0	0.25	Низкая	Неактуальная
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	5	0.5	Средняя	Актуальная
УБИ.036	Угроза исследования механизмов работы программы	10	0.75	Высокая	Актуальная
УБИ.037	Угроза исследования приложения через отчёты об ошибках	5	0.5	Средняя	Актуальная
УБИ.040	Угроза конфликта юрисдикций различных стран	0	0.25	Низкая	Неактуальная
УБИ.041	Угроза межсайтового скриптинга	5	0.5	Средняя	Актуальная
УБИ.043	Угроза нарушения доступности облачного сервера	0	0.25	Низкая	Неактуальная
УБИ.044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	0	0.25	Низкая	Неактуальная
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	0	0.25	Низкая	Неактуальная
УБИ.047	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	0	0.25	Низкая	Неактуальная

Идентификатор угрозы	Наименование угрозы	Y2	Y	Реализуемость	Актуальность
УБИ.048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	0	0.25	Низкая	Неактуальная
УБИ.049	Угроза нарушения целостности данных кеша	10	0.75	Высокая	Актуальная
УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	0	0.25	Низкая	Неактуальная
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	0	0.25	Низкая	Неактуальная
УБИ.055	Угроза незащищённого администрирования облачных услуг	0	0.25	Низкая	Неактуальная
УБИ.056	Угроза некачественного переноса инфраструктуры в облако	0	0.25	Низкая	Неактуальная
УБИ.058	Угроза неконтролируемого роста числа виртуальных машин	0	0.25	Низкая	Неактуальная
УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	0	0.25	Низкая	Неактуальная
УБИ.061	Угроза некорректного задания структуры данных транзакции	10	0.75	Высокая	Актуальная
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	5	0.5	Средняя	Актуальная
УБИ.063	Угроза некорректного использования функционала программного обеспечения	5	0.5	Средняя	Актуальная
УБИ.064	Угроза некорректной реализации политики лицензирования в облаке	0	0.25	Низкая	Неактуальная
УБИ.065	Угроза неопределённости в распределении ответственности между ролями в облаке	0	0.25	Низкая	Неактуальная
УБИ.066	Угроза неопределённости ответственности за обеспечение безопасности облака	0	0.25	Низкая	Неактуальная
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	5	0.5	Средняя	Актуальная
УБИ.069	Угроза неправомерных действий в каналах связи	0	0.25	Высокая	Неактуальная
УБИ.070	Угроза непрерывной модернизации облачной инфраструктуры	0	0.25	Низкая	Неактуальная
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации	10	0.75	Высокая	Актуальная
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	10	0.75	Высокая	Актуальная
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	10	0.75	Высокая	Актуальная
УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи	0	0.25	Низкая	Неактуальная
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	0	0.25	Низкая	Неактуальная

Идентификатор угрозы	Наименование угрозы	Y2	Y	Реализуемость	Актуальность
УБИ.077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	0	0.25	Низкая	Неактуальная
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	0	0.25	Низкая	Неактуальная
УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	0	0.25	Низкая	Неактуальная
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	0	0.25	Низкая	Неактуальная
УБИ.080	Угроза несанкционированного доступа к сегментам вычислительного поля	0	0.25	Низкая	Неактуальная
УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	0	0.25	Низкая	Неактуальная
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	0	0.25	Низкая	Неактуальная
УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	0	0.25	Низкая	Неактуальная
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	10	0.75	Высокая	Актуальная
УБИ.088	Угроза несанкционированного копирования защищаемой информации	5	0.5	Средняя	Актуальная
УБИ.089	Угроза несанкционированного редактирования реестра	5	0.5	Средняя	Актуальная
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	5	0.5	Средняя	Актуальная
УБИ.091	Угроза несанкционированного удаления защищаемой информации	5	0.5	Средняя	Актуальная
УБИ.093	Угроза несанкционированного управления буфером	10	0.75	Высокая	Актуальная
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием	10	0.75	Высокая	Актуальная
УБИ.095	Угроза несанкционированного управления указателями	10	0.75	Высокая	Актуальная
УБИ.096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	0	0.25	Низкая	Неактуальная
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	10	0.75	Высокая	Актуальная
УБИ.099	Угроза обнаружения хостов	10	0.75	Высокая	Актуальная
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	5	0.5	Средняя	Актуальная
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные	5	0.5	Средняя	Актуальная
УБИ.103	Угроза определения типов объектов защиты	10	0.75	Высокая	Актуальная
УБИ.104	Угроза определения топологии вычислительной сети	10	0.75	Высокая	Актуальная
УБИ.109	Угроза перебора всех настроек и параметров приложения	5	0.5	Средняя	Актуальная
УБИ.111	Угроза передачи данных по скрытым каналам	10	0.75	Высокая	Актуальная

Идентификатор угрозы	Наименование угрозы	Y2	Y	Реализуемость	Актуальность
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	0	0.25	Средняя	Актуальная
УБИ.114	Угроза переполнения целочисленных переменных	0	0.25	Низкая	Неактуальная
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	10	0.75	Высокая	Актуальная
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	10	0.75	Высокая	Актуальная
УБИ.117	Угроза перехвата привилегированного потока	10	0.75	Высокая	Актуальная
УБИ.118	Угроза перехвата привилегированного процесса	10	0.75	Высокая	Актуальная
УБИ.119	Угроза перехвата управления гипервизором	0	0.25	Низкая	Неактуальная
УБИ.120	Угроза перехвата управления средой виртуализации	0	0.25	Низкая	Неактуальная
УБИ.121	Угроза повреждения системного реестра	5	0.5	Средняя	Актуальная
УБИ.122	Угроза повышения привилегий	10	0.75	Высокая	Актуальная
УБИ.124	Угроза подделки записей журнала регистрации событий	5	0.5	Средняя	Актуальная
УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	0	0.25	Низкая	Неактуальная
УБИ.126	Угроза подмены беспроводного клиента или точки доступа	0	0.25	Низкая	Неактуальная
УБИ.128	Угроза подмены доверенного пользователя	10	0.75	Высокая	Актуальная
УБИ.130	Угроза подмены содержимого сетевых ресурсов	10	0.75	Высокая	Актуальная
УБИ.133	Угроза получения сведений о владельце беспроводного устройства	0	0.25	Низкая	Неактуальная
УБИ.134	Угроза потери доверия к поставщику облачных услуг	0	0.25	Низкая	Неактуальная
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако	0	0.25	Низкая	Неактуальная
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	10	0.75	Высокая	Актуальная
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	5	0.5	Средняя	Актуальная
УБИ.145	Угроза пропуска проверки целостности программного обеспечения	10	0.75	Высокая	Актуальная
УБИ.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	0	0.25	Низкая	Неактуальная
УБИ.147	Угроза распространения несанкционированно повышенных прав на всю грид-систему	0	0.25	Низкая	Неактуальная
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов	10	0.75	Высокая	Актуальная
УБИ.150	Угроза сбоя процесса обновления BIOS	10	0.75	Высокая	Актуальная
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	0	0.25	Низкая	Неактуальная
УБИ.152	Угроза удаления аутентификационной информации	5	0.5	Средняя	Актуальная
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	10	0.75	Высокая	Актуальная

Идентификатор угрозы	Наименование угрозы	Y2	Y	Реализуемость	Актуальность
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	10	0.75	Высокая	Актуальная
УБИ.155	Угроза утраты вычислительных ресурсов	10	0.75	Высокая	Актуальная
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	5	0.5	Средняя	Актуальная
УБИ.158	Угроза форматирования носителей информации	5	0.5	Средняя	Актуальная
УБИ.159	Угроза «форсированного веб-браузинга»	0	0.25	Низкая	Неактуальная
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	5	0.5	Средняя	Актуальная
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	5	0.5	Средняя	Актуальная
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	10	0.75	Высокая	Актуальная
УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	0	0.25	Низкая	Неактуальная
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов	10	0.75	Высокая	Актуальная
УБИ.166	Угроза внедрения системной избыточности	5	0.5	Средняя	Актуальная
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам	0	0.25	Низкая	Неактуальная
УБИ.169	Угроза наличия механизмов разработчика	10	0.75	Высокая	Актуальная
УБИ.170	Угроза неправомерного шифрования информации	10	0.75	Высокая	Актуальная
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	10	0.75	Высокая	Актуальная
УБИ.172	Угроза распространения «почтовых червей»	10	0.75	Высокая	Актуальная
УБИ.173	Угроза «спама» веб-сервера	0	0.25	Низкая	Неактуальная
УБИ.174	Угроза «фарминга»	10	0.75	Высокая	Актуальная
УБИ.175	Угроза «фишинга»	10	0.75	Высокая	Актуальная
УБИ.176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты	0	0.25	Низкая	Неактуальная
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	5	0.5	Средняя	Актуальная
УБИ.179	Угроза несанкционированной модификации защищаемой информации	5	0.5	Средняя	Актуальная
УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	0	0.25	Низкая	Неактуальная
УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	0	0.25	Низкая	Неактуальная
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	0	0.25	Низкая	Неактуальная
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	0	0.25	Низкая	Неактуальная
УБИ.188	Угроза подмены программного обеспечения	5	0.5	Средняя	Актуальная
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	5	0.5	Средняя	Актуальная

Идентификатор угрозы	Наименование угрозы	Y2	Y	Реализуемость	Актуальность
УБИ.192	Угроза использования уязвимых версий программного обеспечения	5	0.5	Средняя	Актуальная
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	0	0.25	Низкая	Неактуальная
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	0	0.25	Низкая	Неактуальная
УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	0	0.25	Низкая	Неактуальная
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	5	0.5	Средняя	Актуальная
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	0	0.25	Низкая	Неактуальная
УБИ.212	Угроза перехвата управления информационной системой	0	0.25	Низкая	Неактуальная