ДЕПАРТАМЕНТ СПОРТА ТОМСКОЙ ОБЛАСТИ

ПРИКАЗ

28.07.2025 № 33

О постоянно действующей рабочей группе по формированию Перечня недопустимых событий для обеспечения непрерывности операционной деятельности при использовании информационных технологий в Департаменте спорта Томской области

В целях выработки комплексного решения по управлению информационной безопасностью, повышения надежности операционной деятельности при использовании информационных технологий в Департаменте спорта Томской области, в соответствии с методическими рекомендациями по формированию перечня недопустимых событий для обеспечения непрерывности операционной деятельности организаций при выполнении показателей оперативного рейтинга эффективности и результативности ответственных за цифровую трансформацию, разработанными Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации

ПРИКАЗЫВАЮ:

1. Создать постоянно действующую рабочую группу по формированию перечня недопустимых событий для обеспечения непрерывности операционной деятельности при использовании информационных технологий в Департаменте спорта Томской области (далее - рабочая группа) и утвердить ее состав согласно приложению № 1.

2. Утвердить Положение о постоянно действующей рабочей группе по формированию перечня недопустимых событий для обеспечения непрерывности операционной деятельности при использовании информационных технологий в Департаменте спорта Томской области согласно приложению № 2.

3. Контроль за исполнением настоящего приказа оставляю за собой.

4. Настоящий приказ вступает в силу со дня его официального опубликования.

Начальник Департамента М.В. Максимов

Департамент спорта Для документов Томской области

Государственная регистрация
Дата: 01.08.2025
Номер: 876-39/2025

Приложение № 1
к приказу Департамента спорта Томской области
от 28.07.2025 № 33

Состав
постоянно действующей рабочей группы по формированию Перечня недопустимых событий для обеспечения непрерывности операционной деятельности при использовании информационных технологий в Департаменте спорта Томской области

Роговцев Станислав Владимирович	- заместитель начальника Департамента - председатель комитета физической культуры, спорта и цифрового развития, руководитель группы;
Иванов Алексей Сергеевич	- заместитель начальника Департамента - председатель комитета стратегического и бюджетного планирования, член рабочей группы;
Санникова Елена Валерьевна	- председатель комитета организационно-правового обеспечения, член рабочей группы;
Пилипенко Наталья Владимировна	- председатель комитета экономики и финансов - главный бухгалтер, член рабочей группы;
Маковкин Владимир Иванович	- консультант комитета организационно-правового обеспечения, член рабочей группы (с функцией секретаря).

Приложение № 2
к приказу Департамента спорта Томской области
от 28.07.2025 № 33

Положение
о постоянно действующей рабочей группе по формированию перечня недопустимых событий для обеспечения непрерывности операционной деятельности при использовании информационных технологий в Департаменте спорта Томской области

1. Общие положения

1.1. Положение о постоянно действующей рабочей группе по формированию перечня недопустимых событий для обеспечения непрерывности операционной деятельности при использовании информационных технологий в Департаменте спорта Томской области (далее - Положение) определяет порядок работы постоянно действующей рабочей группы по формированию перечня недопустимых событий для обеспечения непрерывности операционной деятельности при использовании информационных технологий в Департаменте спорта Томской области (далее - рабочая группа).

1.2. Основные понятия, используемые в настоящем Положении, приведены в приложении № 1.

1.3. Для обеспечения непрерывности операционной деятельности при использовании информационных технологий в Департаменте спорта Томской области (далее – Департамент) необходимо:

регламентировать технологические процессы;

для каждого технологического процесса определить показатели надежности операционной деятельности и соблюдать их;

сформировать перечень недопустимых событий.

1.4. В целях формирования перечня недопустимых событий создается рабочая группа.

1.5. Руководство рабочей группой возлагается на заместителя начальника Департамента - председателя комитета физической культуры, спорта и цифрового развития.

1.6. К отдельным этапам работ, указанным в разделе 2 настоящего Положения, допускается привлечение представителей экспертных организаций, имеющих лицензию Федеральной службы по техническому и экспортному контролю на осуществление деятельности по технической защите конфиденциальной информации и (или) аккредитованных Федеральной службой безопасности Российской Федерации на выполнение работ по обнаружению, предупреждению и ликвидации последствий компьютерных атак (либо имеющих соответствующее соглашение с Национальным координационным центром по

компьютерным инцидентам) (далее - эксперты), а также представителей разработчиков программного обеспечения и поставщиков информационно-телекоммуникационного оборудования.

1.7. Вспомогательными материалами для определения недопустимых событий могут являться отраслевые и общегосударственные перечни недопустимых событий, сведения об основных показателях эффективности деятельности Департамента, результаты оценки рисков недопустимых событий, результаты стратегического планирования и анализа внешней среды, система менеджмента качества Департамента, элементы технологических процессов и критичных информационных систем.

2. Этапы работы рабочей группы

Рабочая группа осуществляет следующие этапы работы:

2.1. Формирование перечня последствий реализации недопустимых событий и их ранжирование по степени значимости для деятельности Департамента.

В рамках данного этапа выполняются следующие мероприятия:

определение неприемлемых и нежелательных видов ущерба для Департамента;

рассмотрение антропогенных причин возникновения недопустимых событий и отбор последствий реализации недопустимых событий, характерных для Департамента;

формулирование метрики измерения недопустимых событий и оценки критичности недопустимых событий, при превышении которой ущерб считается неприемлемым, для каждого идентифицированного последствия реализации недопустимого события;

отбор наиболее критичных последствий реализации недопустимых событий, оценка критичности ущерба от которых потенциально может достигать неприемлемое значение (пороговое значение).

2.2. Определение технологических процессов и связанных с ними информационных систем.

При формировании перечня недопустимых событий необходимо учесть критичные последствия реализации рисков, связанные с технологическими процессами, где они могут возникнуть, дополнить перечень технологических процессов возможными недостатками их функционирования, а также указать целевые информационные системы и применяемые или планируемые к внедрению контрольные и защитные меры информационной безопасности.

2.3. Формирование гипотетических сценариев реализации недопустимых событий.

В рамках данного этапа выполняются следующие мероприятия:

определение действий, направленных на информационные системы, и создание сценариев реализации недопустимых событий, приводящих к критичным последствиям (далее - сценарии). Сценарии должны имитировать действия злоумышленников, пытающихся достичь целевых информационных

систем. Сценарии должны быть реалистичными и применимыми к информационным системам Департамента;

разработка проекта перечня недопустимых событий согласно приложению № 2 на основе списка сценариев. Для определения недопустимых событий можно использовать методы выявления корневых причин и группировки по однородным признакам.

2.4. Определение критериев реализации недопустимых событий.

В рамках данного этапа выполняются следующие мероприятия:

оценка каждого сценария с учетом потенциальной возможности проведения компьютерных атак при участии специалистов в области информационных технологий и информационной безопасности, которые осуществляют эксплуатацию и техническую поддержку целевых информационных систем и других объектов информационной инфраструктуры;

формирование критериев, подтверждающих возможность реализации недопустимых событий и возникновения критичных последствий реализации недопустимых событий, по результатам анализа сценария для каждой целевой информационной системы.

2.5. Моделирование сценариев.

Для оценки реализуемости сценариев рекомендуется проводить практическую имитацию компьютерных атак с привлечением экспертов. В случае непредвиденных сценариев перечень недопустимых событий дополняется, проводится оценка последствий реализации рисков и определяется критерий реализации недопустимых событий.

2.6. Формирование перечня недопустимых событий.

Рабочая группа формирует итоговый перечень недопустимых событий, в котором указываются критерии реализации недопустимых событий и целевые информационные системы, а также информация об уязвимостях, мерах защиты, квалификации персонала и готовности к угрозам безопасности информации.

Перечень недопустимых событий утверждается руководителем рабочей группы.

Верифицированный и утвержденный перечень недопустимых событий используется для разработки мер по предотвращению наступления недопустимых событий, а также повышению защищенности и обеспечению информационной безопасности Департамента.

Актуализация перечня недопустимых событий проводится при изменении профилей риска Департамента в зависимости от влияния внешних факторов, при изменении информационно-технологического ландшафта Департамента, при появлении новых или исключении действующих технологических процессов Департамента, при появлении достоверных сведений о новых методах кибератак, которые могут быть применены для реализации недопустимых событий.

Верификация недопустимых событий и актуализация перечня недопустимых событий проводится не реже одного раза в год.

3. Структура и порядок деятельности рабочей группы

3.1. Рабочая группа состоит из руководителя рабочей группы и иных членов рабочей группы.

3.2. Руководитель рабочей группы председательствует на заседаниях рабочей группы, определяет перечень вопросов, выносимых на рассмотрение рабочей группы, дату, время и место проведения заседания рабочей группы, осуществляет контроль за выполнением принятых рабочей группой решений.

3.3. Секретарь рабочей группы осуществляет подготовку материалов к заседаниям рабочей группы, оформляет протоколы заседаний рабочей группы, выполняет иные поручения руководителя рабочей группы.

3.4. В состав рабочей группы входят должностные лица Департамента, ответственные за:

управление рисками и обеспечение непрерывности деятельности;

сопровождение и развитие информационных технологий;

обеспечение информационной безопасности.

3.5. Заседания рабочей группы могут проходить в формате стратегических сессий, совещаний, круглых столов и мозговых штурмов.

3.6. Заседание рабочей группы является правомочным, если на нем присутствует не менее половины от общего числа лиц, входящих в состав рабочей группы.

3.7. Решения рабочей группы принимаются простым большинством голосов присутствующих на заседании рабочей группы лиц, входящих в состав рабочей группы, и оформляются протоколом заседания рабочей группы в течение трех рабочих дней со дня проведения заседания рабочей группы.

3.8. В случае равенства голосов решающим является голос председательствующего на заседании рабочей группы.

3.9. Протокол заседания рабочей группы подписывает председательствующий на заседании рабочей группы.

Приложение № 1
к Положению

Основные понятия, используемые в Положении о постоянно действующей рабочей группе по формированию перечня недопустимых событий для обеспечения непрерывности операционной деятельности при использовании информационных технологий
в Департаменте спорта Томской области

1. Антропогенные причины недопустимого события - лица (группа лиц), осуществляющие реализацию рисков информационной безопасности путем несанкционированного доступа и (или) воздействия на информационные ресурсы и (или) компоненты систем и сетей.

2. Вектор компьютерной атаки - последовательность действий злоумышленника в рамках компьютерной атаки, произведенная им в отношении определенного набора ресурсов автоматизированной информационной системы и позволившая ему получить определенный уровень доступа (привилегий) на этих ресурсах.

3. Компьютерная атака - целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.

4. Критерий реализации недопустимого события - факт, технологическое условие или граничные значения длительности, масштаба или сценария воздействия (либо промежуточного результата), отражающий условие и возможность реализации варианта недопустимого события в повседневной операционной деятельности организации (например, факт получения максимальных привилегий в прикладном программном обеспечении на целевой информационной системе в результате реализации вектора компьютерной атаки). Метрика, которая позволяет однозначно подтвердить и зафиксировать наступление недопустимого события в отличие от инцидента информационной безопасности.

5. Недопустимое событие - отдельное событие, цепочка или сочетание событий, вызванных компьютерной атакой, в результате которых прерывается операционная деятельность организации.

6. Непрерывность операционной деятельности организации - способность организации обеспечить стабильное функционирование и развитие своей деятельности при использовании информационных технологий.

7. Последствия реализации недопустимых событий - все виды ущерба и убытков организации, региона, отрасли, государства, вызванные реализацией рисков информационной безопасности вследствие компьютерной атаки на объекты информационной инфраструктуры, приводящие к прерыванию операционной деятельности организации.

8. Целевая информационная система - информационная система, в результате воздействия злоумышленника на которую может наступить недопустимое событие.

9. Целевой сегмент сети - сегмент сети организации, в котором расположена целевая информационная система.

Приложение № 2
к Положению

ПЕРЕЧЕНЬ
недопустимых событий

N п/п	Наименование недопустимого события	Пороговое значение недопустимого события	Наименование целевой информационной системы	Сценарий реализации недопустимого события	Критерий реализации недопустимого события
1.					
...					