Министерство по физической культуре и спорту Челябинской области
ОБЛАСТНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ «РЕГИОНАЛЬНЫЙ ЦЕНТР СПОРТИВНОЙ ПОДГОТОВКИ ПО ДЗЮДО ЧЕЛЯБИНСКОЙ ОБЛАСТИ ИМЕНИ ЗАСЛУЖЕННОГО ТРЕНЕРА РОССИИ А.Е.МИЛЛЕРА»
(ОБУ «РЦСП по дзюдо Челябинской области имени А.Е. Миллера»)

Приложение 11

УТВЕРЖДЕН
приказом директора
ОБУ «РЦСП по дзюдо
Челябинской области
имени А.Е. Миллера»

от 30.03.2023 № 125-ОД

г.Челябинск

РЕГЛАМЕНТ
по выявлению инцидентов информационной безопасности и реагирования на них в областном бюджетном учреждении «Региональный центр спортивной подготовки по дзюдо Челябинской области имени Заслуженного тренера России А.Е. Миллера»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий регламент разработан в целях организации работ по выявлению инцидентов информационной безопасности(далее – инцидентов ИБ) и реагирования на них, в соответствии подпунктом 6 пункта 2 статьи 19 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ.

1.2. Регламент рассматривает вопросы обнаружения, идентификации, анализа инцидентов, планирования и принятия мер по их устранению, а также планирования и принятия мер по предотвращению повторного возникновения инцидентов в областном бюджетном учреждении «Региональный центр спортивной подготовки по дзюдо Челябинской области имени Заслуженного тренера России А.Е.Миллера» (далее - ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера»).

1.3. Организацию работ по реагированию на инцидент, его локализацию, ликвидацию (минимизацию) ущерба, непосредственные работы по выявлению, реагированию, ликвидации и выработке мер для исключения проявления инцидента в дальнейшем, выполняет ответственный за обеспечение безопасности персональных данных в информационных системах (далее – ответственный за обеспечение безопасности ПДн в ИС).

1.4. Ответственный за обеспечение безопасности ПДн назначается приказом ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера»).

1.5. В случае необходимости, в рамках реагирования и расследования инцидента ответственный за обеспечение безопасности ПДн вправе опрашивать работников ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера».

II. ПОНЯТИЕ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Инцидентом называется нежелательное или неожиданное событие в системе защиты информации, которое подвергает риску информационные ресурсы и (или) системы, вызвать сбой в работе оборудования, а также может поставить под угрозу систему защиты информации в ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера».

2.2. Инцидентом, в общем случае, называется любое нарушение применяемых ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера» организационно-технических мер по защите информации.

2.3. Инциденты возникают в процессе противоправных действий злоумышленника, направленных на получение контроля над информационными ресурсами и (или) системами ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера».

2.4. Инцидент ИБ может произойти как в ходе реализации угрозы информационной безопасности, заранее спрогнозированной в модели угроз, так и при помощи других методов, например, методов социальной инженерии, направленных на конкретного пользователя с целью получения информации.

III. ОБНАРУЖЕНИЕ И ИДЕНТИФИКАЦИЯ ИНЦИДЕНТОВ

3.1. Информация об инцидентах может поступать по следующим каналам:

3.1.1. информация, получаемая от работников ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера») в устной либо письменной форме, по телефону, системе электронного документооборота и делопроизводства, официальным письмом и так далее;

3.1.2. журналы регистрации событий сетевого оборудования и межсетевых экранов;

3.1.3. журналы регистрации событий общесистемного программного обеспечения;

3.1.4. журналы регистрации событий прикладного программного обеспечения;

3.1.5. оповещения антивирусных систем;

3.1.6. оповещения систем обнаружения вторжений (атак);

3.1.7. оповещения сканеров уязвимостей;

3.1.8. оповещения других систем.

3.2. Оборудование должно быть настроено таким образом, чтобы ответственный за обеспечение безопасности ПДн смог оперативно получать информацию о произошедших нештатных событиях.

3.3. Общесистемное программное обеспечение, прикладное программное обеспечение и средства защиты информации должны быть настроены таким образом, чтобы обеспечивалось надежное хранение событий информационной безопасности на протяжении не менее 6 месяцев с момента регистрации и исключающим несанкционированное удаление электронных журналов регистрации.

3.4. Работники ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера») при совершении нарушения или при получении информации об инциденте, а также при получении информации обо всех нетипичных событиях, сообщений системы, сообщений систем защиты (например, антивирусной системы) обязаны незамедлительно сообщить о происходящем ответственному за обеспечение безопасности ПДн.

3.5. Информация об инциденте сообщается ответственному за обеспечение безопасности ПДн в произвольной форме и должна содержать следующую информацию:

3.5.1. дата, время обнаружения инцидента;

3.5.2. ФИО лица, сообщившего информацию;

3.5.3. предмет инцидента (например, текст сообщения средства защиты информации, о действиях третьих лиц, направленных на получение доступа к автоматизированному рабочему месту и т.п.).

IV. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

4.1. После получения информации об инциденте ответственный за обеспечение безопасности ПДн должен оперативно провести анализ инцидента и определить категорию инцидента.

4.2. В ходе анализа инцидента определяются:

4.2.1. фактическая или потенциальная возможность реализации угрозы безопасности информации;

4.2.2. опасности угрозы безопасности информации;

4.2.3. перечни информационных ресурсов, затрагиваемые воздействием угрозы безопасности информации;

4.2.4. потенциальные нарушители, цели и причины реализации угрозы безопасности информации;

4.2.5. предварительный перечень мер по локализации и остановке распространения действия угрозы безопасности информации;

4.2.6. оценка последствий инцидента, в том числе возможный или фактический ущерб.

4.3. Оценка последствий инцидента определяется в соответствии с присвоенной категорией инцидента:

- **1 категория.** Инцидент может привести к незначительным негативным последствиям (ущербу) для информационных ресурсов (систем).
- **2 категория.** Инцидент может привести к негативным последствиям (ущербу) для информационных ресурсов (систем).
- **3 категория.** Инцидент может привести к значительным негативным последствиям (ущербу) для информационных ресурсов (систем), деловой репутации ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера».

4.4. В зависимости от присвоенной категории инцидента, ответственный за обеспечение безопасности ПДн определяет приоритет и время реагирования, согласно таблице:

категория инцидента	**приоритет**	**время реагирования, часов, не более**
1	низкий	8
2	средний	4
3	высокий	1

4.5. В случае определения категории 2 и 3 ответственный за обеспечение безопасности ПДн в обязательном порядке доводит информацию об инциденте до директора ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера» и о предложениях по устранению негативных последствий, либо минимизации негативных последствий.

4.6. Первостепенной задачей ответственного за обеспечение безопасности ПДн является сдерживание инцидента, то есть принятие всех необходимых мер для локализации инцидента и препятствующих его распространению.

4.7. В процессе реагирования на инцидент ответственный за обеспечение безопасности ПДн собирает всю информацию для проведения расследования инцидента, планирует и предпринимает меры по устранению инцидентов, в том числе:

4.7.1. по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев;

4.7.2. устранению последствий нарушения правил разграничения доступа;

4.7.3. неправомерных действий по сбору информации;

4.7.4. внедрения вредоносных компьютерных программ (вирусов);

4.7.5. иных событий, приводящих к возникновению инцидентов.

V. РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

5.1. Расследование инцидента информационной безопасности включает проверку и сбор доказательств с технических средств (серверов, сетевых устройств, автоматизированных рабочих мест (далее – АРМ) и т.д.) и без использования технических средств.

5.2. Целью расследования инцидента ИБ является раскрытие всех причинно-следственных связей и получение следующей информации:

5.2.1. источники инцидента ИБ (нарушители);

5.2.2. цели инцидента ИБ (информационные ресурсы, информация ограниченного доступа, персональные данные, репутация, др.);

5.2.3. способы осуществления инцидента ИБ.

5.3. Сбор свидетельств инцидента представляет собой процедуру сбора фактов злонамеренных действий, направленных на реализацию угроз информационной безопасности. Причины, по которым необходим сбор свидетельств, рассматриваются как получение законных оснований для привлечения к ответственности лица или группы лиц за умышленное или непреднамеренное действие (бездействие) или попытку действия, направленную на реализацию угрозы ИБ в информационных системах ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера».

5.4. Основной задачей по расследованию инцидентов ИБ является выявление (идентификация) нарушителя и источника инцидента в целях локализации нарушения и предотвращения дальнейшего распространения инцидента.

5.5. При выявлении нарушителя по инцидентам 3-й категории ответственный за обеспечение безопасности ПДн сообщает директору ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера» об обстоятельствах произошедшего инцидента и предварительных результатах в целях решения вопроса о назначении служебной проверки по фактам инцидента ИБ.

При этом, по поручению директора ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера», ответственный за обеспечение безопасности ПДн незамедлительно принимает меры по отстранению работника ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера» от работы на АРМ, имеющего отношение к инциденту ИБ для исключения дальнейшего развития инцидента и сохранения доказательной базы.

5.6. После выявления нарушителей по инцидентам 2-й и 3-й категории ответственный за обеспечение безопасности ПДн проводит проверку их АРМ.

В ходе проверки проводится анализ:

5.6.1. записей в журналах регистрации событий системы, программного обеспечения (далее – ПО) указывающих на реализацию атаки (угрозы) или неизвестную ранее активность;

5.6.2. историю интернет - обозревателей (включая файлы окружения, такие как cookies), сообщения электронной почты (включая прикрепленные файлы), в т.ч. удаленные;

5.6.3. установленное или записанное ПО, не относящееся к основной деятельности работника ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера»);

5.6.4. наличие подозрительных файлов (включая графические или с незарегистрированными расширениями имен);

5.6.5. проверка возможности у пользователя отключать средства защиты (антивирусная защита, средства НСД, очистка журналов регистрации событий и т.д.);

5.6.6. проверка возможности подключения пользователем неавторизованного носителя информации (в т.ч. соответствие предоставленных прав к информационным ресурсам (системам)), осуществлять загрузку операционной системы с альтернативного носителя и т.д.;

5.6.7. в определенных случаях, например, при явных признаках реализации угрозы данным пользователем, анализ может так же включать поиск удаленных файлов и областей, потерянных кластеров, свободного места, а также восстановление данных с обнаруженных в окружении носителей.

5.7. Ответственный за обеспечение безопасности ПДн в обязательном порядке должен обеспечить надежное хранение свидетельств расследования инцидента в любом виде (электронные журналы регистрации событий, снимки экрана, фотографии и т.д.). Время хранения устанавливается – не менее 2 лет.

5.8. Факт составления ответственным за обеспечение безопасности ПДн акта проведения расследования инцидента является моментом завершения расследования инцидента.

5.9. В акте расследования инцидента указываются обстоятельства и дата возникновения инцидента, участники инцидента (нарушители), последствия и результаты расследования инцидента.

5.10. После проведения расследования инцидента ответственный за обеспечение безопасности ПДн в срок, не превышающий 10 рабочих дней с момента завершения расследования:

5.10.1. проводит переоценку угроз, повлекших возникновение инцидента;

5.10.2. готовит перечень защитных мер для минимизации выявленных рисков, в случае повторения инцидента ИБ;

5.10.3. при необходимости инициирует проведение переработки соответствующих организационно-распорядительной документации в сфере защиты информации, включая настоящий регламент.

VI. ОТВЕТСТВЕННОСТЬ

6.1. Каждый пользователь информационных систем ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера» несет персональную ответственность за:

– свои действия во время информационного взаимодействия в рамках своих служебных обязанностей;

– соблюдение требований, установленных настоящим Регламентом.

6.2. За несоблюдение требований настоящего Регламента, виновные в нарушении работники ОБУ «РЦСП по дзюдо Челябинской области имени А.Е.Миллера», привлекаются к ответственности в соответствии с действующим законодательством Российской Федерации.