



Министерство спорта Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Уральский государственный университет физической культуры»
(ФГБОУ ВО «УралГУФК»)

ПРИКАЗ

№ 93

г. Челябинск

«11» апреля 2015 г.

О сотрудниках, ответственных за выявление компьютерных инцидентов в ФГБОУ ВО «УралГУФК» и реагирование на них.

В целях обеспечения безопасности персональных данных и выполнения требований приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

приказываю:

1. Утвердить перечень сотрудников, ответственных за выявление компьютерных инцидентов и реагирование на них (прилагается).
2. Утвердить регламент выявления компьютерных инцидентов в ФГБОУ ВО «УралГУФК» и реагирования на них (далее – регламент) (прилагается).
3. Сотрудникам, ответственным за выявление компьютерных инцидентов и реагирование на них, в своей деятельности руководствоваться регламентом.
4. Контроль за исполнением настоящего приказа оставляю за собой.

И.о. ректора

Черепов Е.А.

Утверждаю:
И.о. ректора ФГБОУ ВО «УралГУФК»
Е.А. Черепов
18 августа 2015 г.



Регламент выявления компьютерных инцидентов в ФГБОУ ВО «УралГУФК» и реагирования на них

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий регламент выявления компьютерных инцидентов в ФГБОУ ВО «УралГУФК» и реагирования на них (далее – Регламент) разработан с учетом следующих документов:

– Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Политика информационной безопасности в ФГБОУ ВО «УралГУФК»;

– Национальный стандарт РФ ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»;

– Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».

1.2. Целью разработки данного Регламента является установление общих правил, требований и процедур выявления компьютерных инцидентов в системах (сетях) ФГБОУ ВО «УралГУФК» и реагирования на них.

1.3. Под системами (сетями) в рамках настоящего Регламента рассматриваются:

– государственные информационные системы (далее – ГИС);

– информационные системы персональных данных (далее – ИСПДн) с установленным первым, вторым или третьим уровнем защищенности персональных данных;

– информационные системы (далее – ИС) и информационно-телекоммуникационные сети (далее – ИТКС).

1.4. Настоящий Регламент предназначен для сотрудников, ответственных за выявление компьютерных инцидентов ФГБОУ ВО «УралГУФК» и реагирование на них.

1.5. Настоящий Регламент устанавливает:

– основные этапы выявления компьютерных инцидентов и реагирования на них;

– задачи и обязанности группы реагирования на инциденты информационной безопасности, а также ответственность ее участников.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Термины и определения, применяемые для целей настоящего Регламента:

2.1.1. **Группа реагирования на инциденты информационной безопасности (ГРИИБ)** – сотрудник или группа сотрудников ФГБОУ ВО «УралГУФК», назначенные ответственными за выявление компьютерных инцидентов и реагирование на них.

2.1.2. Компьютерная атака – целенаправленное воздействие программных и (или) программно-аппаратных средств на информационную систему, информационно-телекоммуникационные сети, автоматизированную систему управления или сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

2.1.3. Компьютерный инцидент – факт нарушения и (или) прекращения функционирования информационной системы, информационно-телекоммуникационной сети, автоматизированной системы управления или сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

2.1.4. Система защиты информации – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

2.1.5. Событие информационной безопасности (событие ИБ) – идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

3. ВЫЯВЛЕНИЕ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

3.1. Обнаружение и оповещение о событиях ИБ

3.1.1. Обнаружению компьютерного инцидента предшествует обнаружение событий ИБ.

3.1.2. Информация о событиях ИБ может поступать ГРИИБ из различных источников. В качестве таких источников информации, как минимум, следует рассматривать:

- средства защиты информации, входящие в состав систем защиты информации информационных (автоматизированных) систем;
- программное обеспечение информационной (автоматизированной) системы;
- системы мониторинга событий и журналов событий ИБ (при наличии таковых);
- сотрудников ФГБОУ ВО «УралГУФК».

3.1.3. Информация о событии ИБ предоставляется сотрудниками ФГБОУ ВО «УралГУФК» ГРИИБ в свободной форме, если иное не установлено руководителем ФГБОУ ВО «УралГУФК».

3.2. Оценка и принятие решений

3.2.1. Все события ИБ, поступающие ГРИИБ, должны быть рассмотрены ГРИИБ.

3.2.2. В ходе рассмотрения ГРИИБ должна произвести анализ, относится ли событие ИБ к компьютерному инциденту или является ложным. С этой целью ГРИИБ может производить получение любых уточнений от лица, сообщившего о событии ИБ, и собирать

требуемую дополнительную информацию, считающуюся доступной, как от лица, сообщившего о событии ИБ, так и из любого другого источника. Категории компьютерных инцидентов и связанные с ними типы событий информационной безопасности представлены в приложении № 1 к настоящему Регламенту.

3.2.3. По всем событиям ИБ, отнесенным к компьютерным инцидентам, ГРИИБ должна обеспечить:

3.2.3.1. Проведение предварительной оценки последствий компьютерного инцидента. Оценка должна быть проведена в отношении каждого из свойств безопасности информации: конфиденциальности, целостности и доступности. При оценке необходимо руководствоваться следующими правилами:

- если компьютерный инцидент не влечет нарушение свойства безопасности информации, то оценка должна иметь значение «Отсутствует»;

- если компьютерный инцидент влечет нарушение свойства безопасности информации, вследствие чего информационная (автоматизированная) система может выполнять свои функции только с привлечением дополнительных сил и средств, то оценка должна иметь значение «Низкое»;

- если компьютерный инцидент влечет нарушение свойства безопасности информации, вследствие чего информационная (автоматизированная) система не может выполнять свои функции, то оценка должна иметь значение «Высокое».

3.2.3.2. Немедленное уведомление о выявленном компьютерном инциденте любым доступным способом следующих лиц:

- руководителя структурного подразделения (должностного лица (сотрудника)), ответственного за обеспечение безопасности персональных данных и за защиту информации, если компьютерный инцидент выявлен в ГИС и ИСПДн;

- администратора безопасности объектов критической информационной инфраструктуры, если компьютерный инцидент выявлен в ИС, АСУ или ИТКС, являющейся значимым объектом критической информационной инфраструктуры или в отношении которой Ректором ФГБОУ ВО «УралГУФК» принято решение о применении требований по обеспечению безопасности, предусмотренных для значимых объектов критической информационной инфраструктуры (далее – администратор безопасности).

4. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

4.1. Регистрация и уведомление

4.1.1. После подтверждения компьютерного инцидента ГРИИБ выполняет действия по его регистрации, в рамках которой проводится:

- Регистрация в журнале компьютерных инцидентов (приложение 2);

4.2. Анализ и определение действий по реагированию

4.2.1. Анализ компьютерного инцидента проводится с целью определения порядка действий по устранению причин и условий возникновения, а также последствий компьютерного инцидента. В ходе анализа компьютерного инцидента ГРИИБ принимает решение о дальнейших действиях в отношении компьютерного инцидента. Если для принятия решений о дальнейших действиях сведений о компьютерном инциденте

недостаточно, то ГРИИБ может осуществлять сбор дополнительных данных по компьютерному инциденту и связанным с ним событиям ИБ.

4.2.2. В рамках принятия решений о дальнейших действиях ГРИИБ должна:

4.2.2.1. Подготовить порядок локализации (предотвращение дальнейшего распространения компьютерного инцидента) и устранения последствий компьютерного инцидента.

4.2.2.2. Назначить ответственных за локализацию, устранение последствий и сбор доказательств.

4.2.2.3. Определить перечень средств, необходимых для принятия мер по ликвидации последствий компьютерных инцидентов.

4.2.2.4. Определить очередность информационных (автоматизированных) систем и (или) их структурных элементов, в отношении которых будут приниматься меры по ликвидации последствий компьютерного инцидента.

4.2.2.5. Совместно с руководителем ФГБОУ ВО «УралГУФК», руководителем структурного подразделения или должностным лицом (сотрудником), ответственным за обеспечение безопасности персональных данных и за защиту информации принять решение:

- об обращении в сторонние организации с целью их привлечения для реагирования и (или) расследования компьютерного инцидента (в том числе в правоохранительные органы);

- о необходимости сбора доказательств для дальнейшего расследования компьютерного инцидента.

4.2.3. Все решения, принятые в ходе анализа компьютерного инцидента, должны протоколироваться ГРИИБ путем фиксации информации в карточке компьютерного инцидента.

4.3. Устранение причин, условий и последствий

4.3.1. Устранение причин, условий и последствий компьютерного инцидента осуществляется в соответствии с порядком, подготовленным в соответствии с пунктом 4.2.2.1 настоящего Регламента, и направлено на восстановление пораженных информационных (автоматизированных) систем(ы), сервисов(а) и (или) сетей(и) до нормального рабочего состояния.

4.3.2. В случае принятия решения о необходимости сбора доказательств для дальнейшего расследования компьютерного инцидента лица, ответственные за сбор доказательств, должны обеспечить максимально полное документальное фиксирование сведений, которые могут быть связаны с компьютерным инцидентом. К таким сведениям могут относиться:

- сведения об инфраструктуре (параметры настроек аппаратного и программного обеспечения, в том числе средств защиты информации, сведения о составе программного обеспечения);

- журналы системного и прикладного программного обеспечения информационной (автоматизированной) системы;

- журналы информационно-телекоммуникационного оборудования

информационной (автоматизированной) системы;

- журналы регистрации событий безопасности средств защиты информации;
- записи систем видеонаблюдения.

5. АНАЛИЗ И УЛУЧШЕНИЕ

5.1. Расследование компьютерного инцидента

5.1.1. Расследование компьютерного инцидента представляет из себя процесс, в рамках которого осуществляется определение причин возникновения компьютерного инцидента и разработка предложений по улучшению систем защиты информации информационных (автоматизированных) систем с целью исключения появления аналогичных компьютерных инцидентов в будущем.

5.1.2. По усмотрению ГРИИБ расследование компьютерного инцидента может не проводиться.

5.1.3. Как правило, при расследовании инцидента осуществляется:

5.1.3.1. Определение причин и условий возникновения компьютерного инцидента и виновных лиц. В качестве причин возникновения компьютерного инцидента следует рассматривать, как минимум, следующие:

- неудачная и (или) неправильная конфигурация программного обеспечения информационной (автоматизированной) системы, в том числе средств защиты информации;

- отсутствие надлежащего уровня контроля за событиями ИБ и действиями пользователей информационной (автоматизированной) системы;

- умышленные или неумышленные (неосознанные) действия сотрудника ФГБОУ ВО «УралГУФК»;

- низкая осведомленность сотрудников ФГБОУ ВО «УралГУФК» об угрозах безопасности информации и о правилах безопасной работы;

- ненадлежащее исполнение сотрудниками ФГБОУ ВО «УралГУФК» своих должностных обязанностей;

- несвоевременное обновление микропрограммного и программного обеспечения.

5.1.3.2. Определение размера ущерба, нанесенного ФГБОУ ВО «УралГУФК» вследствие компьютерного инцидента. Размер ущерба определяется ГРИИБ совместно с руководителем структурного подразделения или должностным лицом (сотрудником), ответственным за обеспечение безопасности персональных данных и за защиту информации. К оценке нанесенного ущерба могут привлекаться другие сотрудники ФГБОУ ВО «УралГУФК».

5.1.3.3. Определение возможности и целесообразности привлечения виновных лиц к ответственности. В том случае, когда причиной инцидента ИБ послужили действия или бездействие персонала информационной (автоматизированной) системы, необходимо определить возможность и целесообразность привлечения указанных лиц к дисциплинарной или гражданско-правовой ответственности. Решение о привлечении персонала к ответственности принимается руководителем ФГБОУ ВО «УралГУФК» по запросам руководителя структурного подразделения или должностного лица (работника),

ответственного за обеспечение безопасности персональных данных и за защиту информации.

5.1.3.4. Определение путей совершенствования систем защиты информации информационных (автоматизированных) систем.

5.1.4. Информация и действия, совершаемые в ходе расследования компьютерного инцидента, должны быть зафиксированы в карточке компьютерного инцидента.

5.2. Улучшение

5.2.1. Улучшение включает в себя внедрение рекомендаций, сформированных на этапе расследования компьютерного инцидента. Улучшение может включать:

5.2.1.1. Улучшение анализа рисков и менеджмента безопасности; характеризуется внесением изменений в процессы классификации информационных (автоматизированных) систем, анализа угроз безопасности информации и управления процессами обеспечения информационной безопасности. В качестве примера таких изменений можно рассматривать учет новых угроз и уязвимостей.

5.2.1.2. Улучшение безопасности, характеризующееся обновлением (улучшением) уже внедренных или внедрением новых мер защиты информации.

5.2.1.3. Другие улучшения, не отнесенные к пунктам 5.2.1.1 и 5.2.1.2 настоящего Регламента. Например, изменения в политиках, стандартах и процедурах информационной безопасности, а также изменения в конфигурациях аппаратного и программного обеспечения.

6. ОТВЕТСТВЕННОСТЬ

6.1. Сотрудники ФГБОУ ВО «УралГУФК», включенные в состав ГРИИБ, несут персональную ответственность за:

6.1.1. Ненадлежащее исполнение или неисполнение требований, предусмотренных настоящим Регламентом.

6.1.2. Обеспечение безопасного хранения информации о компьютерных инцидентах.

ПРИЛОЖЕНИЕ № 1
к Регламенту выявления компьютерных
инцидентов в ФГБОУ ВО «УралГУФК» и
реагирования на них

**Категории компьютерных инцидентов и связанные с ними типы событий
информационной безопасности**

Категория инцидента и его международное обозначение	Тип события информационной безопасности и его международное обозначение
Заражение вредоносным программным обеспечением (malware)	Внедрение в контролируемый ИР модулей ВПО (malware infection)
Распространение вредоносного программного обеспечения (malware distribution)	Использование контролируемого ИР для распространения ВПО (malware command and control)
	Попытки внедрения модулей ВПО в контролируемый ИР (infection attempt)
Нарушение или замедление работы контролируемого информационного ресурса (availability)	Компьютерная атака типа “отказ в обслуживании”, направленная на контролируемый ИР (dos)
	Распределенная компьютерная атака типа “отказ в обслуживании”, направленная на контролируемый ИР (ddos)
	Несанкционированный вывод ИР из строя (sabotage)
	Непреднамеренное (без злого умысла) отключение ИР (outage)
Несанкционированный доступ в систему (intrusion)	Успешная эксплуатация уязвимости в контролируемом ИР (application compromise)
	Компрометация учетной записи в контролируемом ИР (account compromise)
Попытки несанкционированного доступа в систему или к информации (intrusion attempt)	Попытки эксплуатации уязвимости в контролируемом ИР (exploit attempt)
	Попытки авторизации в контролируемом ИР (login attempt)
Сбор сведений с использованием ИКТ (information gathering)	Сканирование информационного ресурса (scanning)
	Прослушивание (захват) сетевого трафика, контролируемого ИР (traffic hijacking)
	Социальная инженерия, направленная на компрометацию ИР (social engineering)
Нарушение безопасности информации (information content security)	Несанкционированное разглашение информации, обрабатываемой в контролируемом ИР (unauthorised access)
	Несанкционированное изменение информации, обрабатываемой в контролируемом ИР (unauthorised modification)
Распространение информации с неприемлемым содержанием (abusive content)	Рассылка спам-сообщений с контролируемого ИР (spam)
	Публикация в контролируемом ИР запрещенной законодательством РФ информации (prohibited content)
Мошенничество с использованием ИКТ (fraud)	Злоупотребление при использовании ИР (unauthorized purposes)
	Публикация в контролируемом ИР мошеннической информации (phishing)
Уязвимость (vulnerability)	Наличие уязвимости или недостатков конфигурации в ИР (vulnerability)

Журнал компьютерных инцидентов

[illegible]