МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Горно-Алтайский государственный университет»
(ФГБОУ ВО ГАГУ, ГАГУ, Горно-Алтайский государственный университет)

ПРИЛОЖЕНИЕ №1
к приказу №155 от 08.06.2026

РЕГЛАМЕНТ
08.06.2026 № 01-05-61

выявления компьютерных инцидентов и реагирования на них в федеральном государственном бюджетном образовательном учреждении высшего образования «Горно-Алтайский государственный университет»

1. Общие положения

1.1. Настоящий Регламент выявления компьютерных инцидентов и реагирования на них в федеральном государственном бюджетном образовательном учреждении высшего образования
«Горно-Алтайский государственный университет» (далее – Регламент и ГАГУ соответственно) разработан в целях установления общих правил, требований и процедур выявления компьютерных инцидентов в системах (сетях) ГАГУ и реагирования на них.

1.2. Регламент разработан с учетом следующих документов:

– Федерального закона от 08.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Указа Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;

– приказа Федеральной службы по техническому и экспортному контролю от 21.12.2017
№ 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;

– приказа Федеральной службы по техническому и экспортному контролю от 25.12.2017

№ 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

– приказ ФСБ России от 25 декабря 2025 г. № 546 «Об утверждении Порядка обмена информацией о компьютерных атаках и компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты»;

– Национального стандарта Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;

– Национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК ТО 18044-2007
«Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»;

– Национального стандарта Российской Федерации ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей».

1.3. Регламент предназначен для работников ГАГУ, ответственных за выявление, регистрацию компьютерных инцидентов в ГАГУ и реагирование на них, а также работников и обучающихся ГАГУ, использующих информационные ресурсы и системы ГАГУ.

1.4. Регламент устанавливает основные этапы деятельности:

– по обнаружению признаков компьютерных инцидентов, оповещению об инцидентах информационной безопасности, включая компьютерные инциденты, и их оценке;

– организации и контролю процессов реагирования на компьютерные инциденты с привлечением специалистов подразделений, ответственных за эксплуатацию контролируемых информационных ресурсов и (или) непосредственное выполнение действий по реагированию, включая активизацию соответствующих защитных мер для предотвращения, уменьшения последствий и (или) восстановления после негативных воздействий;

– анализу результатов деятельности по управлению компьютерными инцидентами для приобретения и накопления опыта, который может использоваться для предотвращения повторного возникновения компьютерных инцидентов и повышения эффективности процедур реагирования на компьютерные инциденты и актуализации нормативных и методических

документов (политики, регламенты, положения и т.д.) в части управления компьютерными инцидентами и информационной безопасностью ГАГУ в целом;

– извлечению уроков из инцидентов информационной безопасности, введению превентивных защитных мер и улучшению общего подхода к менеджменту инцидентов информационной безопасности.

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

2. Используемые в Регламенте термины и определения

2.1. Администратор безопасности – работник структурного подразделения ГАГУ – владельца информационного ресурса, назначаемый приказом ректора ГАГУ и являющийся ответственным за защиту информационной, автоматизированной системы от несанкционированного доступа к информации, выполняющий работы по поддержанию функционирования системы в рамках выбранной политики безопасности; устранению неполадок; обеспечению должного уровня конфиденциальности и целостности данных; созданию и сохранению резервных копий данных; созданию и поддержанию в актуальном состоянии учётных записей пользователей; отслеживанию информации об уязвимостях системы и своевременному принятию мер по их локализации; документированию работы системы.

Вредоносное программное обеспечение (ВПО) – любое программное обеспечение, предназначенное для осуществления несанкционированного доступа и/или воздействия на информацию или ресурсы информационной системы в обход существующих правил разграничения доступа.

Группа реагирования на инциденты информационной безопасности (ГРИИБ) – работник или группа работников ГАГУ, назначенных ответственными за выявление компьютерных инцидентов, своевременную регистрацию информации о них, реагирование на них и обработку информации во время их жизненного цикла (приложение 1).

Информационный ресурс (ИР) – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

Инцидент информационной безопасности (инцидент ИБ) – появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ.

Критическая информационная инфраструктура (КИИ) – объекты

критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Компьютерная атака (КА) – целенаправленное воздействие программных и (или) программно-аппаратных средств на информационную систему, информационно- телекоммуникационную сеть, 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.

Компьютерный инцидент (КИ) – 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. (Основные категории компьютерных инцидентов приведены в приложении 2.)

Национальный координационный центр по компьютерным инцидентам (НКЦКИ) – обеспечивает координацию деятельности субъектов критической информационной инфраструктуры Российской Федерации по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, в отношении которых проведено категорирование в установленном законодательством Российской Федерации порядке либо принято решение уполномоченным лицом ГАГУ о применении требований по обеспечению безопасности, предусмотренных для объектов критической информационной инфраструктуры.

Системы (сети) – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления (далее – соответственно ИС, ИТКС, АСУ) ГАГУ.

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.

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.

Уязвимость – недостаток программного (программно-технического) средства или информационной системы в целом, который может быть использован для реализации угроз безопасности информации.

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 следует рассматривать:

– уведомления о признаке компьютерного инцидента, направляемые дежурной службой Национального координационного центра по компьютерным инцидентам (НКЦКИ);

– уведомления соответствующих подразделений федеральных органов исполнительной власти, штаба по обеспечению кибербезопасности и центра по противодействию кибератакам Республики Татарстан;

– сообщения администраторов безопасности ИС, АСУ или ИТКС;

– сообщения работников и обучающихся ГАГУ;

– электронные сообщения средств защиты информации, входящих в состав систем защиты информации ИС; системы мониторинга событий и журналов событий ИБ (при наличии таковых);

– электронные журналы программного обеспечения ИС;

– электронные банки данных угроз безопасности информации, базы угроз и уязвимостей программного обеспечения.

3.1.3. Информация о событии ИБ предоставляется в ГРИИБ с использованием корпоративной электронной почты на адрес ob@gasu.ru.

3.2. Оценка значимости последствий компьютерного инцидента и принятие решений

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

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 уточнять сведения у лица, сообщившего о событии ИБ, и собирать требуемую дополнительную информацию, считающуюся доступной, из любого другого источника.

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

3.2.3.1. Проведение предварительной оценки значимости 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 ИС 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 ИС не может выполнять свои функции, то оценка должна иметь значение
«Высокое».

3.2.3.2. Незамедлительное уведомление о выявленном компьютерном инциденте любым доступным способом администратора безопасности ИС, АСУ или ИТКС, если компьютерный инцидент выявлен в ИС, АСУ или ИТКС, являющейся объектом (в том числе значимым) критической информационной инфраструктуры или в отношении которой уполномоченным лицом ГАГУ принято решение о применении требований по обеспечению безопасности, предусмотренных для значимых объектов критической информационной инфраструктуры.

4. Реагирование на компьютерные инциденты

4.1. Регистрация компьютерного инцидента и уведомление подразделений, задействованных в устранении последствий

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

– заведение карточки компьютерного инцидента либо запись в журнале учета компьютерных атак и уязвимостей, компьютерных инцидентов (приложение 3 к Регламенту); ввод в базу данных (при наличии) компьютерных инцидентов;

– информирование НКЦКИ в соответствии с требованиями к внешнему взаимодействию при обеспечении безопасности КИИ (в случае выявления на объекте КИИ).

4.2. Анализ компьютерного инцидента и определение действий по реагированию на него

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 осуществляет сбор дополнительных данных по компьютерному инциденту и связанных с ним событий ИБ.

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

4.2.2.1. Предложить порядок локализации компьютерного инцидента (предотвращения дальнейшего распространения компьютерного инцидента) и устранения его последствий.

4.2.2.2. Определить ответственных за локализацию компьютерного инцидента, устранение его последствий и сбор и обобщение информации о сущности компьютерного инцидента.

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

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

4.2.2.5. Совместно с администратором безопасности ИС, АСУ или ИТКС ГАГУ принять решение:

4.2.3. об информировании руководства ГАГУ, об обращении в сторонние организации с целью их привлечения для реагирования и (или) расследования компьютерного инцидента (в том числе в правоохранительные органы);

4.2.4. о необходимости дальнейшего сбора материала и документирования информации о сущности компьютерного инцидента для расследования.

4.2.5. Все решения, принятые в ходе анализа компьютерного инцидента, должны протоколироваться ГРИИБ путем фиксации информации в журнале учета компьютерных атак и уязвимостей, компьютерных инцидентов.

4.3. Устранение причин, условий и последствий компьютерного инцидента

4.3.1. Устранение причин, условий и последствий компьютерного инцидента осуществляется в соответствии с пунктом 4.2.2 Регламента и направлено на восстановление пораженных ИС, сервисов(а) и (или) сетей(и) до нормального рабочего состояния.

4.3.2. В случае принятия решения о необходимости дальнейшего сбора материала и документирования информации о сущности компьютерного инцидента, ответственные лица 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);

– электронные журналы системного и прикладного программного обеспечения ИС; информационно-телекоммуникационного оборудования ИС; регистрации событий безопасности средств защиты информации;

– записи систем видеонаблюдения.

4.3.3. О результатах мероприятий по реагированию на компьютерный инцидент и принятию мер по ликвидации последствий компьютерных атак ГРИИБ должна проинформировать НКЦКИ в срок не позднее 48 часов после завершения таких мероприятий в соответствии с требованиями к внешнему взаимодействию при обеспечении безопасности КИИ.

5. Анализ и совершенствование деятельности по выявлению КИ и реагированию на них

5.1. Расследование компьютерного инцидента

5.1.1. Расследование компьютерного инцидента представляет собой процесс, в рамках которого осуществляется определение причин возникновения компьютерного инцидента и разработка предложений по улучшению систем защиты информации ИС, с целью исключения появления аналогичных компьютерных инцидентов в будущем.

5.1.2. По решению 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, например:

– неудачную и (или) неправильную конфигурацию программного обеспечения ИС, в том числе средств защиты информации;

– отсутствие надлежащего контроля за событиями ИБ и действиями пользователей ИС;

– умышленные или неумышленные (неосознанные) действия работников ГАГУ;

– низкую осведомленность работников ГАГУ об угрозах безопасности информации и правилах безопасной работы;

– несвоевременное обновление микропрограммного и программного обеспечения.

5.1.3.2. Определение размера ущерба, нанесенного ГАГУ вследствие компьютерного инцидента.

Размер ущерба определяется ГРИИБ совместно с администратором безопасности. К оценке нанесенного ущерба могут привлекаться специалисты всех (отдельных) структурных подразделений ГАГУ.

5.1.3.3. Определение возможности и целесообразности привлечения виновных лиц к ответственности.

В случае если причиной инцидента ИБ послужили действия или бездействие персонала ИС, необходимо определить целесообразность привлечения указанных лиц к ответственности за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Регламентом, в пределах, определенных действующим трудовым законодательством Российской Федерации. Решение о привлечении к ответственности принимается ректором ГАГУ по запросам ГРИИБ.

5.1.3.4. Определение путей совершенствования систем защиты информации ИС.

5.1.4. Информация и действия, совершаемые в ходе расследования компьютерного инцидента, должны быть зафиксированы в карточке компьютерного инцидента либо в журнале учета компьютерных атак и уязвимостей, компьютерных инцидентов.

5.2. Совершенствование деятельности по выявлению КИ и реагированию на них

Совершенствование деятельности включает в себя внедрение рекомендаций, сформированных на этапах устранения причин, последствий и расследования компьютерного инцидента:

5.2.1. Совершенствование анализа рисков и менеджмента безопасности. Характеризуется внесением изменений в процессы классификации ИС, анализа угроз безопасности информации и управления процессами обеспечения информационной безопасности. В качестве примера таких изменений можно рассматривать учет новых угроз и уязвимостей.

5.2.2. Совершенствование системы безопасности. Характеризуется обновлением имеющихся или внедрением новым мер защиты информации.

5.2.3. Другие мероприятия, не отнесенные к пунктам 5.2.1 и 5.2.2 настоящего Регламента, например, изменения в политиках, стандартах и процедурах информационной безопасности, а также изменения в конфигурациях аппаратного и программного обеспечения.

6. Ответственность за исполнение настоящего Регламента

6.1. Работники, включенные в состав ГРИИБ, несут персональную ответственность за правонарушения, совершенные в процессе осуществления своей деятельности, в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации, и за

ненадлежащее исполнение или неисполнение требований, предусмотренных Регламентом, и необеспечение безопасной обработки и хранения информации о компьютерных инцидентах – в пределах, определенных действующим трудовым законодательством Российской Федерации.

7. Заключительные положения

7.1. Журнал учета компьютерных атак и уязвимостей, компьютерных инцидентов может вестись ГРИИБ в электронном виде при принятии соответствующих мер по обеспечению его сохранности и предоставлению полного доступа к информации, содержащейся в нем, только работникам, входящим в ГРИИБ.

7.2. Срок хранения журнала учета компьютерных атак и уязвимостей, компьютерных инцидентов – три года.

7.3. Информация из журнала учета компьютерных атак и уязвимостей, компьютерных инцидентов предоставляется в ходе проверок подразделениям федеральных органов исполнительной власти, реализующих государственную политику в сфере информационной безопасности, а также по запросам правоохранительных органов. Информация в отношении конкретных инцидентов предоставляется также работникам ГАГУ и третьим лицам, привлекаемым к проведению мероприятий по локализации, устранению последствий компьютерных инцидентов и сбору доказательств.

8. Внесение изменений в Регламент

8.1. Внесение изменений и дополнений в настоящий Регламент осуществляется путем утверждения его в новой редакции или путем издания приказа ГАГУ о внесении изменений и дополнений в настоящий Регламент.

Приложение №1
к регламенту
выявления компьютерных инцидентов и реагирования на них в
федеральном государственном бюджетном образовательном учрежденим
высшего образования «Горно-Алтайский государственный университет»

Работники ГАГУ, входящие в состав группы реагирования на инциденты информационной безопасности (ГРИИБ)

№ п/п	Структурное подразделение	Должность	Функции
1.	Центр цифрового развития	Руководитель	Координация деятельности по реагированию на компьютерные инциденты. Определение приоритетов реагирования. Организация взаимодействия с внешними организациями, включая НКЦКИ.
2.	Центр цифрового развития	Начальник отдела сетевого и системного администрирования	Обнаружение компьютерных атак и регистрация компьютерных инцидентов. Первичная обработка информации об инцидентах. Передача информации ответственным лицам для реагирования.
3.	Управление комплексной безопасности	Начальник	Организация деятельности по защите информации и реагированию на компьютерные инциденты. Координация мероприятий по предотвращению компьютерных атак и ликвидации их последствий. Взаимодействие с внешними организациями и государственными структурами.
4.	Управление комплексной безопасности	Специалист по ИБ	Мониторинг событий информационной безопасности. Регистрация компьютерных инцидентов и ведение учета. Реагирование на инциденты и участие в ликвидации их последствий. Эксплуатация средств обнаружения компьютерных атак и систем управления событиями информационной безопасности.

5.	Управление по правовой и кадровой работе	Начальник	Правовое сопровождение реагирования на компьютерные инциденты. Подготовка правовых документов и материалов при взаимодействии с государственными органами и организациями.

Приложение №2
к регламенту
выявления компьютерных инцидентов и реагирования на них в
федеральном государственном бюджетном образовательном учрежденим
высшего образования «Горно-Алтайский государственный университет»

Основные 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 контролируемую систему (сеть) модулей ВПО (malware infection)
Распространение вредоносного программного обеспечения (Malware distribution)	Использование контролируемой системы (сети) для распространения ВПО (malware command and control)
	Попытки внедрения модулей ВПО в контролируемую систему (сеть) (infection attempt)
Нарушение или замедление работы контролируемого информационного ресурса (Availability)	Компьютерная атака типа «отказ в обслуживании», направленная на контролируемую систему (сеть) (dos)
	Распределенная компьютерная атака типа «отказ в обслуживании», направленная на контролируемую систему (сеть) (ddos)
	Несанкционированный вывод контролируемой системы (сети) из строя (sabotage)
	Непреднамеренное (без злого умысла) отключение контролируемой системы (сети) (outage)
Несанкционированный доступ в систему (Intrusion)	Успешная эксплуатация уязвимости в контролируемой системе (сети) (application compromise)
	Компрометация учетной записи в контролируемой системе (сети) (account compromise)
Попытки несанкционированного доступа в систему или к информации (Intrusion attempt)	Попытки эксплуатации уязвимости в контролируемой системе (сети) (exploit attempt)
	Попытки авторизации в контролируемой системе (сети) (login attempt)
Сбор сведений с использованием ИКТ (Information gathering)	Сканирование контролируемой системы (сети) (scanning)
	Прослушивание (захват) сетевого трафика контролируемой системы (сети) (traffic hijacking)
	Социальная инженерия, направленная на компрометацию контролируемой системы (сети) (social engineering)
Нарушение безопасности информации (Information content security)	Несанкционированное разглашение информации, обрабатываемой в контролируемой системе (сети) (unauthorised access)
	Несанкционированное изменение информации, обрабатываемой контролируемой системой (в сети) (unauthorised modification)
Распространение информации с неприемлемым содержимым (Abusive content)	Рассылка спам-сообщений контролируемой системой (из сети) (spam)
	Публикация в контролируемой системе (сети) запрещенной законодательством Российской Федерации информации (prohibited content)
Мошенничество с использованием ИКТ (Fraud)	Злоупотребление при использовании контролируемой системы (сети) (unauthorized purposes)
	Публикация в контролируемой системе (сети) мошеннической информации (phishing)
Уязвимость (Vulnerability)	Наличие уязвимости или недостатков конфигурации контролируемой системы (сети) (vulnerability)

Приложение №3
к регламенту
выявления компьютерных инцидентов и реагирования на них в
федеральном государственном бюджетном образовательном учрежденим
высшего образования «Горно-Алтайский государственный университет»

ЖУРНАЛ
учета компьютерных атак и уязвимостей, компьютерных инцидентов

(учет карточек КА/признака КИ и уязвимостей, работниками и обучающимися ГАГУ)

№	Наименование объекта	Категория значимости объекта	Местонахождение объекта	Учетный номер формы	Тип компьютерной атаки/уязвимости	Объект компьютерной атаки	Дата и время компьютерной атаки	IP-адрес субъекта (источника) компьютерной атаки	Принятые меры по устранению последствий компьютерной атаки	Нанесенный ущерб	Время простоя	Оповещенные работники		Дата и время оповещения НКЦКИ	Примечание
												подразде-ление	Ф.И.О.		
1.															