ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ НОВОСИБИРСКОЙ ОБЛАСТИ "НОВОСИБИРСКИЙ ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ"

Подписано цифровой подписью: ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ НОВОСИБИРСКОЙ ОБЛАСТИ "НОВОСИБИРСКИЙ ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ"
DN: c=RU, st=Новосибирская область, street=г. Новосибирск, ул. Немировича-Данченко, 121, l=Новосибирск, title=Директор, o=ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ НОВОСИБИРСКОЙ ОБЛАСТИ "НОВОСИБИРСКИЙ ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ", 1.2.643.100.1=120D313032353430313330373132 38, 1.2.643.100.3=120B303732333038363838383631, 1.2.643.100.4=120A353430333130373535 36, 1.2.643.3.131.1.1=120C353430373234353733383 837, email=it-config2012@mail.ru, givenName=Светлана Сергеевна, sn=Лузан, cn=ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ НОВОСИБИРСКОЙ ОБЛАСТИ "НОВОСИБИРСКИЙ ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ"
Дата: 2026.05.14 15:27:33 +07'00'

УТВЕРЖДАЮ
Директор государственного бюджетного профессионального образовательного учреждения Новосибирской области «Новосибирский профессионально-педагогический колледж»
_____ С.С. Лузан

приказ от 12.05.2026 № 200 – о.д.

Регламент выявления компьютерных инцидентов и реагирования на них

Новосибирск 2026

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент выявления компьютерных инцидентов и реагирования на них в ГБПОУ НСО «НППК» (далее – Регламент) устанавливает общие правила и порядок выявления компьютерных инцидентов и реагирования на них в ГБПОУ НСО «НППК» (далее – Колледж).

1.2. Основания разработки настоящего Регламента:

– приказ Федеральной службы по техническому и экспортному контролю России 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»;

– приказ Федеральной службы по техническому и экспортному контролю России от 21 декабря 2017 г. №235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;

– приказ Федеральной службы по техническому и экспортному контролю России от 25 декабря 2017 г. №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

– приказ Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений »;

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

– положение об обеспечении безопасности значимых объектов критической информационной инфраструктуры ГБПОУ НСО «НППК»;

– стандарт защиты информации в ГБПОУ НСО «НППК».

1.3. Настоящий Регламент обязателен к применению в отношении следующих объектов информатизации:

– информационные системы, включенные в соответствии с Политикой защиты информации в ГБПОУ НСО «НППК» в перечень объектов, подлежащих защите в Колледже в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;

– значимые объекты критической информационной инфраструктуры;

– объекты критической информационной инфраструктуры, в отношении которых Колледжом принято решение о применении требований по обеспечению безопасности, предусмотренных для значимых объектов критической информационной инфраструктуры;

– информационные системы персональных данных с установленным первым или вторым уровнем защищенности персональных данных.

1.4. Регламент обязателен для применения:

– всеми сотрудниками Колледжа, включенными в состав группы реагирования на инциденты информационной безопасности;

– подрядными организациями при их привлечении к мероприятиям по выявлению компьютерных инцидентов и реагирования на них.

1.5. Все сотрудники Колледжа и работники подрядных организаций должны быть ознакомлены с настоящим Регламентом.

1.6. Регламент подлежит пересмотру и, при необходимости, изменению в следующих случаях:

– при изменении законодательства Российской Федерации в области выявления компьютерных инцидентов и реагирования на них;

– при внедрении рекомендаций по улучшению менеджмента компьютерных инцидентов, сформированных по результатам произошедшего компьютерного инцидента.

1.7. Внесение изменений (корректировок) в настоящий Регламент осуществляется путем утверждения его новой редакции.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В настоящем Регламенте используются следующие основные термины и определения

2.1.1. **Группа реагирования на компьютерные инциденты (ГРКИ)** – группа лиц (из числа сотрудников Колледжа и (или) работников подрядных организаций), на которую возложены обязанности (функции) по выявлению компьютерных инцидентов и реагированию 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. **Национальный координационный центр по компьютерным инцидентам (НКЦКИ)** – организация, созданная федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, для обеспечения координации деятельности субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

2.1.5. **Объект информатизации** – информационная система, автоматизированная систему управления, информационно-телекоммуникационная сеть или иной объект информатизации Колледжа;

2.1.6. **Пользователь** – сотрудник Колледжа или иной организации (в том числе подрядной), обладающий правом доступа к информационной системе и (или) содержащейся в ней информации и ее использованию.

2.1.7. **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;

2.1.8. **Событие безопасности** – событие, связанное с возможным нарушением безопасности информации, нарушением функционирования объекта информатизации, реализацией угроз безопасности информации.

2.1.9. **Специалист по защите информации** – должностное лицо Института, выполняющее непосредственные функции по защите информации.

3. ВЫЯВЛЕНИЕ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

3.1. Обнаружение и оповещение о событиях безопасности

3.1.1. Обнаружению компьютерного инцидента предшествует обнаружение события безопасности.

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

– средства защиты информации;

– программное обеспечение;

– системы мониторинга событий и журналов событий безопасности;

– сотрудников Института.

3.1.3. Информация о событии безопасности предоставляется сотрудниками Института ГРКИ в свободной форме.

3.2. Оценка и принятие решений

3.2.1. Все поступающие в ГРКИ события безопасности должны быть рассмотрены.

3.2.2. В ходе рассмотрения ГРКИ должна произвести анализ, относится ли событие безопасности к компьютерному инциденту или является ложным. С этой целью ГРКИ может производить получение любых уточнений от лица, сообщившего о событии безопасности, и собирать требуемую дополнительную информацию, считающуюся доступной, как от лица, сообщившего о событии безопасности, так и из любого другого источника. Категории компьютерных инцидентов и связанные с ними типы событий безопасности представлены в ПРИЛОЖЕНИИ № 1 к настоящему Регламенту.

3.2.3. По всем событиям безопасности, отнесенным к компьютерным инцидентам, ГРКИ 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 объект информатизации 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 объект информатизации не может выполнять свои функции, то оценка должна иметь значение «Высокое».

3.2.3.2 Немедленное уведомление о выявленном компьютерном инциденте любым доступным способом лиц, в зоне ответственности которых находится объект информатизации, связанный с компьютерным инцидентом.

4. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

4.1. Регистрация и уведомление

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

– заведение карточки компьютерного инцидента;

– введение сведений в базу данных компьютерных инцидентов – запись в журнале компьютерных инцидентов;

– информирование НКЦКИ о компьютерном инциденте в соответствии с порядком и требованиями, изложенными в локальных актах Колледжа: Положении о внешнем взаимодействии при обеспечении безопасности критической информационной инфраструктуры, Регламенте взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

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 ГРКИ принимает решение о дальнейших действиях в отношении компьютерного инцидента. Если для принятия решений о дальнейших действиях сведений о компьютерном инциденте недостаточно, то ГРКИ может осуществлять сбор дополнительных данных по компьютерному инциденту и связанным с ним событиям безопасности.

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

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

4.2.2.2 Определить лиц, 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 объектов информатизации и (или) их структурных элементов, в отношении которых будут приниматься меры по ликвидации последствий компьютерного инцидента.

4.2.2.5 Совместно с руководством Колледжа и специалистами по защите 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 ГРКИ 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 объектов информатизации 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 (сведения о составе и параметры настроек программного и программно-аппаратного обеспечения, в том числе средств защиты информации);

– журналы системного и прикладного программного обеспечения;

– журналы оборудования корпоративной среды передачи данных;

– журналы 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, связанных со значимым объектом критической информационной инфраструктуры, ГРКИ должна проинформировать НКЦКИ в срок не позднее 48 часов после завершения таких мероприятий в соответствии с порядком и требованиями, изложенными в Положении о внешнем взаимодействии при обеспечении безопасности критической информационной инфраструктуры.

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 объекта информатизации с целью исключения появления аналогичных компьютерных инцидентов в будущем.

5.1.2. По усмотрению ГРКИ 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, в том числе средств защиты информации;

– отсутствие надлежащего уровня контроля за событиями безопасности и действиями пользователей;

– умышленные или неумышленные (неосознанные) действия пользователя;

– низкая осведомленность пользователя об угрозах безопасности информации и о правилах безопасной работы;

– ненадлежащее исполнение пользователями своих обязанностей;

– несвоевременное обновление программного обеспечения.

5.1.3.2 Определение размера ущерба, нанесенного Колледжу вследствие компьютерного инцидента. Размер ущерба определяется ГРКИ совместно с руководством Колледжа, специалистами по защите информации и лицами, в зоне ответственности которых находится объект информатизации, на котором произошел компьютерный инцидент. К оценке нанесенного ущерба могут привлекаться другие сотрудники Колледжа.

5.1.3.3 Определение возможности и целесообразности привлечения виновных лиц к ответственности. В том случае, когда причиной компьютерного инцидента послужили действия или бездействие пользователей, необходимо определить возможность и целесообразность привлечения указанных лиц к дисциплинарной или гражданско-правовой ответственности. Решение о привлечении сотрудника Колледжа к ответственности принимается руководством Колледжа.

5.1.3.4 Определение путей совершенствования систем защиты информации объектов информатизации.

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 анализа угроз безопасности информации и управления процессами обеспечения защиты информации. В качестве примера таких изменений можно рассматривать учет новых угроз и уязвимостей.

5.2.1.2 Улучшение безопасности: характеризуется 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 защиты информации, а также изменения в конфигурациях программного и программно-аппаратного обеспечения.

ПРИЛОЖЕНИЕ № 1
к Регламенту выявления компьютерных
инцидентов и реагирования на них

Типы событий безопасности, относящиеся к компьютерным инцидентам

– Использование контролируемого ресурса для проведения атак;
– Замедление работы ресурса в результате DDoS-атаки;
– Заражение ВПО;
– Захват сетевого трафика;
– Компрометация учетной записи;
– Несанкционированное изменение информации;
– Несанкционированное разглашение информации;
– Публикация на ресурсе запрещенной законодательством РФ информации;
– Событие не связано с компьютерной атакой;
– Успешная эксплуатация уязвимости.

Лист ознакомления
с Регламентом выявления компьютерных инцидентов и реагирования на них

№ п/п	ФИО	Должность	Дата	Подпись