

## **РЕГЛАМЕНТ**

### **реагирования на инциденты информационной безопасности в информационных системах ФГБОУ ВО «Новосибирская государственная консерватория имени М.И. Глинка»**

#### **1. Общие положения**

1.1. Настоящий Регламент реагирования на инциденты информационной безопасности (далее – Регламент) в информационных системах ФГБОУ ВО «Новосибирская государственная консерватория имени М.И. Глинка» (далее – Консерватория), разработан в соответствии с законодательством Российской Федерации об информации ограниченного доступа (далее – ИОД) и нормативно-методическими документами федеральных органов исполнительной власти по вопросам безопасности ИОД при ее обработке в информационных системах (далее – ИС).

1.2. Настоящий Регламент определяет:

- порядок регистрации событий безопасности;
- порядок выявления инцидентов информационной безопасности и реагированию на них;
- порядок проведения анализа инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов.

1.3. Инцидент информационной безопасности – одно событие или группа событий, которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности ИОД.

1.4. Регламент обязателен для исполнения всеми сотрудниками Консерватории, непосредственно осуществляющими защиту ИОД.

#### **2. Порядок регистрации событий безопасности**

2.1. Регистрация событий безопасности в ИС, осуществляется в следующей последовательности:

- 1) Определение событий безопасности, подлежащих регистрации, и сроков их хранения.
- 2) Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.
- 3) Сбор, запись и хранение информации о событиях безопасности.
- 4) Реагирование на сбор при регистрации событий безопасности.
- 5) Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.
- 6) Генерирование временных меток и (или) синхронизация системного времени в ИС.
- 7) Защита информации о событиях безопасности.

2.2. События безопасности, подлежащие регистрации в ИС, должны определяться с учетом способов реализации угроз безопасности ИОД для ИС. К событиям безопасности, подлежащим регистрации в ИС, должны быть отнесены любые проявления состояния ИС и ее системы защиты информации (далее – СИЗИ), указывающие на возможность нарушения конфиденциальности, целостности или доступности ИОД, доступности компонентов ИС, нарушения процедур, установленных организационно-распорядительными документами по защите информации, а также на нарушение штатного функционирования средств защиты информации (далее – СЗИ).

2.3. События безопасности, подлежащие регистрации в ИС, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов информационной безопасности, возникших в ИС.

2.4. В ИС подлежат регистрации следующие события:

- вход (выход), а также попытки входа субъектов доступа в ИС и загрузки (остановки) операционной системы (далее – ОС);
- подключение съемных машинных носителей ИОД и вывод ИОД на носители ИОД;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой ИОД;
- попытки доступа программных средств к определяемым защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;
- попытки удаленного доступа.

2.5. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъекта доступа (пользователя и (или) процесса), связанного с данным событием безопасности.

2.6. При регистрации входа (выхода) субъектов доступа в ИС и загрузки (остановки) ОС состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (остановки) ОС, результат попытки входа (успешная или неуспешная), результат попытки загрузки (остановки) ОС (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

2.7. При регистрации подключения съемных машинных носителей ИОД и вывода информации на носители ИОД состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения съемных машинных носителей ИОД и вывода ИОД на носители ИОД, логическое имя (номер) подключаемого съемного машинного носителя ИОД, идентификатор субъекта доступа, осуществляющего вывод ИОД на носитель ИОД.

2.8. При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой ИОД состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

2.9. При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

2.10. При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер)).

2.11. При регистрации попыток удаленного доступа к ИС состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к ИС.

2.12. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать:

- возможность выбора ответственным за защиту информации в ИС, подлежащих регистрации в текущий момент времени из перечня событий безопасности определенных в пункте 2.4 настоящего Регламента;
- генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с составом и содержанием информации, определенными в соответствии с пунктами 2.6 – 2.11 настоящего Регламента;
- хранение информации о событиях безопасности в течение времени, установленного в пункте 2.3 настоящего Регламента.

2.13. Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с пунктами 2.7 – 2.11 настоящего Регламента, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

2.14. В ИС должно осуществляться реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.

2.15. Реагирование на сбои при регистрации событий безопасности должно предусматривать:

- предупреждение (сигнализация, индикация) о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;
- реагирование на сбои при регистрации событий безопасности путем изменения ответственным за защиту информации в ИС и (или) администратором ИС параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов ИС, запись поверх устаревших хранимых записей событий безопасности.

2.16. Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации в соответствии и с периодичностью, установленной оператором, и обеспечивающей своевременное выявление признаков инцидентов информационной безопасности в ИС.

2.17. В случае выявления признаков инцидентов информационной безопасности в ИС осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности в соответствии с порядком проведения разбирательств по фактам возникновения инцидентов в ИС.

2.18. Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ИС достигается посредством применения внутренних системных часов ИС.

2.19. Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

2.20. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам:

- ответственному за защиту информации в ИС;
- администратору ИС.

### **3. Порядок выявления инцидентов информационной безопасности и реагирования на них**

3.1. За выявление инцидентов информационной безопасности и реагирование на них отвечают:

- ответственный за защиту информации в ИС;
- администратор ИС.

3.2. Работники организации, должны сообщать ответственным за выявление инцидентов информационной безопасности, любые инциденты, в которые входят:

- факты попыток и успешной реализации несанкционированного доступа в системы обработки информации, в помещения обработки информации и к хранилищам информации;
- факты сбоя или некорректной работы систем обработки информации;
- факты сбоя или некорректной работы СЗИ;
- факты разглашения ИОД;
- факты разглашения информации о методах и способах защиты и обработки информации.

3.3. Все нештатные ситуаций, факты вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки информации в информационной системе должны быть занесены ответственными за выявление инцидентов информационной безопасности в «Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки информации в информационных системах», форма которого приведена в Приложении №1.

3.4. Анализ инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов, осуществляется согласно порядку проведения разбирательств по фактам возникновения инцидентов информационной безопасности в ИС.

3.5. Меры по устранению последствий инцидентов информационной безопасности, планированию и принятию мер по предотвращению повторного возникновения инцидентов, возлагаются на ответственных за выявление инцидентов.

#### **4. Порядок проведения разбирательств по фактам возникновения инцидентов информационной безопасности**

4.1. Для проведения разбирательств по фактам возникновения инцидентов информационной безопасности создается комиссия, состоящая не менее чем из трех человек с обязательным включением в её состав:

- ответственного за защиту информации в ИС;
- администратора ИС.

4.2. Председатель комиссии организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками структурных подразделений организации, готовит и ведёт заседания комиссии, подписывает протоколы заседаний. По окончании работы комиссии готовится заключение по результатам проведенного разбирательства, которое передается на рассмотрение ректору Консерватории.

4.3. При проведении разбирательства устанавливаются:

- наличие самого факта совершения инцидента информационной безопасности, служащего основанием для вынесения соответствующего решения;
- время, место и обстоятельства возникновения инцидента, а также оценка его последствий;
- конкретный работник, совершивший инцидент информационной безопасности или повлекший своими действиями возникновение инцидента;
- наличие и степень вины работника, совершившего инцидент информационной безопасности или повлекшего своими действиями возникновение инцидента;
- цели и мотивы, способствовавшие совершению инцидента информационной безопасности.

4.4. В целях проведения разбирательства все работники обязаны по первому требованию членов комиссии предъявить для проверки все числящиеся за ними материалы и документы, дать устные или письменные объяснения об известных им фактах по существу заданных им вопросов.

4.5. Работник, совершивший инцидент информационной безопасности или повлекший своими действиями возникновение инцидента, обязан по требованию комиссии представить объяснения в письменной форме не позднее трех рабочих дней с момента получения соответствующего требования. Комиссия вправе поставить перед работником перечень вопросов, на которые работник обязан ответить. В случае отказа работника от письменных объяснений, комиссией составляется акт.

4.6. Работник имеет право, по согласованию с председателем комиссии, ознакомиться с материалами разбирательства, касающимися лично его, и давать по поводу них свои комментарии, предоставлять дополнительную информацию и документы. По окончании разбирательства работнику для ознакомления предоставляется итоговый акт с выводами комиссии.

4.7. В случае давления на работника со стороны других лиц (не из состава комиссии) в виде просьб, угроз, шантажа и др., по вопросам, связанным с проведением разбирательства, работник обязан сообщить об этом председателю комиссии.

4.8. До окончания работы комиссии и вынесения решения членам комиссии запрещается разглашать сведения о ходе проведения разбирательства и ставшие известные им обстоятельства.

4.9. В процессе проведения разбирательства комиссией выясняются:

- перечень разглашенных сведений;
- причины разглашения ИОД;
- лица, виновные в разглашении ИОД;
- размер (экспертную оценку) причиненного ущерба;
- недостатки и нарушения, допущенные работниками при работе с ИОД;
- иные обстоятельства, необходимые для определения причин разглашения ИОД, степени виновности отдельных лиц, возможности применения к ним мер воздействия.

4.10. По завершении разбирательства комиссией составляется заключение. В заключении указываются:

- основание для проведения разбирательства;
- состав комиссии и время проведения разбирательства;
- сведения о времени, месте и обстоятельствах возникновения инцидента информационной безопасности;
- сведения о работнике, совершившем инцидент информационной безопасности или повлекшем своими действиями возникновение инцидента (должность, фамилия, имя, отчество, год рождения, время работы в учреждении, а также в занимаемая должность);
- цели и мотивы работника, способствовавшие совершению инцидента информационной безопасности;
- причины и условия возникновения инцидента информационной безопасности;
- данные о характере и размерах причиненного в результате инцидента ущерба;
- предложения о мере ответственности работника, совершившего инцидент информационной безопасности или повлекшего своими действиями возникновение инцидента.

4.11. На основании заключения выносится решение о применении мер ответственности к работнику, совершившему инцидент или повлекшему своими действиями возникновение инцидента, также о возмещении ущерба виновным работником (или его законным представителем), которое доводится до указанного работника в письменной форме под расписку.

4.12. Все материалы разбирательства относятся к ИОД и хранятся в течение 5 лет. Копии заключения и распоряжения по результатам разбирательства приобщаются к личному делу работника, в отношении которого оно проводилось.

### **5. Ответственность**

5.1. Все сотрудники, осуществляющие защиту ИОД, обрабатываемую в ИС, обязаны ознакомиться с данным Регламентом под роспись.

5.2. Сотрудники несут персональную ответственность за выполнение требований настоящего Регламента.

### **6. Срок действия и порядок внесения изменений**

6.1. Настоящий Регламент вступает в силу с момента его утверждения и действует бессрочно.

6.2. Настоящий Регламент подлежит пересмотру не реже одного раза в три года.

6.3. Изменения и дополнения в настоящий Регламент вносятся приказом ректора Консерватории.

