

Утвержден
приказом директора
КОГПОБУ «ОВСХК»
от «10» января 2022г. № 3/18



**Регламент
реагирования на инциденты безопасности**

РЕГЛАМЕНТ
реагирования на инциденты информационной безопасности в
информационных системах персональных данных
КОГПОБУ «ОВСХК»

1.1. Регламент реагирования на инциденты информационной безопасности в информационных системах персональных данных КОГПОБУ «ОВСХК» (далее - регламент), разработан в соответствии с Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных»; постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; приказом ФСТЭК 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»; постановлением Правительства Российской Федерации от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; на основании Устава и локальных нормативных актов КОГПОБУ «ОВСХК» (далее - Колледж).

1.2. В целях реализации настоящего регламента используются следующие термины и их определения:

1.2.1. Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.2.2. Инцидент информационной безопасности - любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

1.2.3. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.2.4. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.2.5. Средство защиты информации - программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

1.3. Настоящий регламент утверждается приказом директора.

1.4. Изменения и дополнения в настоящий регламент утверждаются приказом директора.

1.5. Настоящий регламент является локальным нормативным актом, регламентирующим деятельность Колледжа.

1.6. Срок действия настоящего регламента не ограничен и действует до принятия нового регламента.

1.7. Настоящий регламент подлежит пересмотру не реже одного раза в три года.

2. Общие положения

2.1. 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.

2.2. Регламент обязателен для исполнения всеми работниками Колледжа, непосредственно осуществляющими защиту персональных данных в информационных системах.

3. Инциденты информационной безопасности

3.1. К инцидентам ИБ относятся:

- несоблюдение требований по защите персональных данных:
 - использование ЭВМ в целях, не связанных с выполнением трудовых (служебных, должностных, функциональных) обязанностей;
 - утрата носителя персональных данных;
- утрата ключевых документов, ключей от помещений и хранилищ, личных печатей.
- попытки несанкционированного доступа к персональным данным:

- подбор чужого идентификатора и пароля, последующий доступ с использованием чужого пароля;
 - изменение настроек, состава, паролей технических средств информационных систем персональных данных;
 - изменение (увеличение) полномочий доступа;
 - нарушение целостности установленных защитных пломб;
 - копирование персональных данных на неучтенные съемные носители;
 - заражение рабочего места и/или сервера вредоносной программой;
 - хищение носителей персональных данных;
 - хищение технических средств информационных систем персональных данных;
 - умышленное нарушение работоспособности технических средств;
 - хищение криптосредств, ключевых документов, ключей от помещений и хранилищ, личных печатей;
 - несанкционированное проникновение в помещения информационных систем;
 - очистка электронных журналов мониторинга;
 - сбои в работе технических средств информационных систем персональных данных.
- 3.2. К инцидентам ИБ не относятся:
- неудачные попытки вторжений, которые были обнаружены и нейтрализованы с использованием СЗИ;
 - неудачные попытки заражения рабочих мест и/или серверов вредоносной программой, которые были обнаружены и нейтрализованы с использованием СЗИ.

4. Порядок регистрации событий безопасности

4.1. Регистрация событий безопасности в информационных системах персональных данных 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 сбои 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 информационных системах персональных данных.
- 7) Защита информации о событиях безопасности.

4.2. События безопасности, подлежащие регистрации в информационных системах персональных данных, должны определяться с учетом способов реализации угроз безопасности персональных данных для информационных систем. К событиям безопасности, подлежащим регистрации в информационных системах персональных данных, должны быть отнесены любые проявления состояния ее системы защиты, указывающие на возможность нарушения конфиденциальности, целостности или

доступности персональных данных, доступности компонентов, нарушения процедур, установленных организационно-распорядительными документами по защите персональных данных, а также на нарушение штатного функционирования средств защиты информации (далее - СЗИ).

4.3. События безопасности, подлежащие регистрации в информационных системах персональных данных, и сроки хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов информационной безопасности, возникших в информационных системах.

4.4. В информационных системах персональных данных подлежат регистрации следующие события:

- вход (выход), а также попытки входа субъектов доступа в информационные системы и загрузки (остановка) операционной системы;
- подключение съемных машинных носителей персональных данных и вывод персональных данных на носители;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой персональных данных;
- обновление или ошибки при обновлении программных средств информационных систем и СЗИ;
- 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.

4.5. 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.

4.6. При регистрации входа (выхода) субъектов доступа в информационные системы персональных данных и загрузки (остановка) операционной системы состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (остановки) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (остановка) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

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

4.8. При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой персональных данных 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).

4.9. 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).

4.10. 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)).

4.11. При регистрации попыток удаленного доступа к информационным системам персональных данных 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 информационным системам.

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

- возможность выбора ответственным за обеспечение безопасности персональных данных в информационных системах и (или) Администратором событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в пункте 4.4 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 4.6 - 4.11 настоящего регламента;
- хранение информации о событиях безопасности в течение времени, установленного в пункте 4.3 настоящего регламента.

4.13. 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 4.7 - 4.11 настоящего регламента, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

4.14. В информационных системах персональных данных 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.

4.15. 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 обеспечение безопасности персональных данных в информационных системах и (или) Администратором параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационных систем, запись поверх устаревших хранимых записей событий безопасности.

4.16. 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 информационных системах.

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

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

4.19. 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.

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

- ответственному за обеспечение безопасности персональных данных в информационных системах;
- администратору.

5. Порядок выявления инцидентов информационной безопасности и реагирования на них

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

- ответственный за обеспечение безопасности персональных данных в информационных системах;
- администратор.

5.2. Работники Колледжа, должны сообщать ответственным за выявление инцидентов информационной безопасности о любых инцидентах, в которые входят:

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

5.3. Все нештатные ситуации, факты вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки персональных данных в информационных системах 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 персональных данных в Центре», форма которого установлена в Приложении 1 к настоящему регламенту или в электронные журналы операционной системы и СЗИ.

5.4. 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 информационных системах персональных данных.

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

6. Основные этапы процесса реагирования на инциденты

6.1. Лица, занимающиеся реагированием на инциденты должны обеспечить защиту информационных систем персональных данных и проинформировать пользователей, о важности мер по обеспечению информационной безопасности.

6.2. Лица, занимающиеся реагированием на инциденты, должны определить, является ли обнаруженное ими с помощью различных систем обеспечения информационной безопасности событие инцидентом или нет. Для этого могут использоваться публичные отчеты, потоки данных об угрозах, средства статического и динамического анализа образцов программного обеспечения и другие источники информации. Статический анализ выполняется без непосредственного запуска исследуемого образца и позволяет выявить различные индикаторы, например, строки, содержащие URL-адреса или адреса электронной почты. Динамический анализ подразумевает выполнение исследуемой программы в защищенной среде (Песочнице) или на изолированной машине с целью выявления поведения образца и сбора артефактов его работы.

6.3. Лица, занимающиеся реагированием на инциденты, должны

идентифицировать скомпрометированные компьютеры и настроить правила безопасности таким образом, чтобы заражение не распространилось дальше по сети. Кроме того, на этом этапе необходимо перенастроить сеть таким образом, чтобы информационные системы персональных данных могли продолжать работать без зараженных машин.

6.4. Далее лица, занимающиеся реагированием на инциденты, удаляют вредоносное программное обеспечение, а также все артефакты, которые оно могло оставить на зараженных компьютерах.

6.5. Ранее скомпрометированные компьютеры вводятся обратно в сеть. При этом лица, занимающиеся реагированием на инциденты, некоторое время продолжают наблюдать за состоянием этих машин и информационными системами в целом, чтобы убедиться в полном устранении угрозы.

6.6. Лица, занимающиеся реагированием на инциденты, анализируют произошедший инцидент, вносят необходимые изменения в конфигурацию программного обеспечения и оборудования, обеспечивающего информационной безопасности, и формируют рекомендации для того, чтобы в будущем предотвратить подобные инциденты. При невозможности полного предотвращения будущей атаки составленные рекомендации позволят ускорить реагирование на подобные инциденты.

7. Порядок проведения разбирательств по фактам возникновения инцидентов информационной безопасности

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

- ответственного за обеспечение безопасности персональных данных в информационных системах;
- администратора информационных систем.

7.2. 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 проведённого разбирательства, которое передается на рассмотрение директору Колледжа.

7.3. 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.

7.4. 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.

7.5. 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.

7.6. Работник имеет право, по согласованию с председателем комиссии, знакомиться 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.

7.7. 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.

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

7.9. В процессе проведения разбирательства комиссией выясняются:

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

7.10. 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 Колледже, 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 возникновения инцидента.

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

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

8. Ответственность

8.1. Все работники, осуществляющие защиту персональных данных, обязаны ознакомиться с данным регламентом под подпись.

8.2. Работники несут персональную ответственность за выполнение требований настоящего регламента.