Приложение №1
к приказу от «25» 10 2024 г. № 209

РЕГЛАМЕНТ
реагирования на инциденты информационной безопасности в информационных системах СПбГИПСР

1. Термины и определения

1.1. Информационная система – совокупность содержащихся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

1.2. 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.

1.3. 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;

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

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

1.6. ГосСОПКА – государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак.

2. Общие положения

2.1. Настоящий Регламент реагирования на инциденты информационной безопасности (далее – Регламент) в информационных системах СПбГИПСР (далее – Учреждение), 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).

2.2. Настоящий Регламент определяет:

- порядок регистрации событий безопасности;
- порядок выявления и идентификации инцидентов информационной безопасности, в т.ч. отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа,

неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– порядок информирования пользователями и администраторами лиц, ответственных за выявление инцидентов, и реагирования на них;

– порядок проведения анализа инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

– порядок планирования и принятия мер по устранению инцидентов, в том числе по восстановлению ИС в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– порядок планирования и принятия мер по предотвращению повторного возникновения инцидентов.

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

2.4. Регламент обязателен для исполнения всеми работниками Учреждения, непосредственно осуществляющими защиту ИОД.

3. Инциденты информационной безопасности

3.1. К инцидентам ИБ относятся:

– несоблюдение требований по защите ИОД:

- использование ЭВМ в целях, не связанных с выполнением трудовых (служебных, должностных, функциональных) обязанностей;
- утрата носителя информации;
- утрата ключевых документов, ключей от помещений и хранилищ, личных печатей, удостоверений, пропусков.

– попытки НСД к ИОД:

- подбор чужого идентификатора и пароля, последующий доступ с использованием чужого пароля;
- изменение настроек, состава, паролей технических средств ИС;
- изменение (увеличение) полномочий доступа;
- нарушение целостности установленных защитных пломб;
- копирование ПДн на неучтенные съемные носители информации;
- заражение рабочего места ИС вредоносной программой;
- хищение носителей информации;
- хищение технических средств ИС;
- умышленное нарушение работоспособности технических средств ИС;
- хищение криптосредств, ключевых документов, ключей от помещений и хранилищ, личных печатей, удостоверений, пропусков;
- несанкционированное проникновение в помещения ИС;
- очистка электронных журналов мониторинга.

– сбои в работе технических средств ИС Учреждения.

3.2. К инцидентам ИБ не относятся:

– неудачные попытки вторжений, которые были обнаружены и нейтрализованы с использованием СЗИ;

– неудачные попытки заражения рабочего места ИС вредоносной программой, которые были обнаружены и нейтрализованы с использованием СЗИ.

4. Порядок регистрации событий безопасности

4.1. 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 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 ИС.

7) Защита информации о событиях безопасности.

4.2. 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).

4.3. 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.

4.4. В ИС подлежат регистрации следующие события:

– вход (выход), а также попытки входа субъектов доступа в ИС и загрузки (останова) 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.

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

4.7. 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.

4.8. 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).

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 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.

4.12. 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 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 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.

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 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.

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 ИС.

4.17. В случае выявление 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.

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

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 защиту информации в ИС;
- администратору ИС.

5. Порядок выявления и идентификации инцидентов информационной безопасности

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

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

5.2. 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.

5.3. Все нештатные ситуации, 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 к настоящему Регламенту.

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 ИС.

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

6. Основные этапы процесса реагирования на инциденты

6.1. Лица, занимающиеся реагированием на инциденты, должны обеспечить защиту ИС 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 ИС Учреждения 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 в ИС Учреждения.

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 ИС 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 анализа инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий

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 защиту информации в ИС;
- администратора ИС.

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 ректору Учреждения.

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 возникновения 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 возникновения 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 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.

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

– основание для проведения в 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 возникновения 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 возникновения инцидента.

7.11. 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.

7.12. 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.

8. Порядок реагирования на инциденты, повлекшие неправомерную передачу (предоставление, распространение, доступ) персональных данных

8.1. К инцидентам, повлекшим неправомерную передачу (предоставление, распространение, доступ) персональных данных могут относиться:

- разглашение ПДн;
- несанкционированный доступ к ПДн;
- превышение полномочий сотрудников;
- внедрение вредоносного программного обеспечения;
- компрометация учетных записей.

8.2. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Работники, осуществляющие защиту ПДн обязаны с момента выявления такого инцидента Оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных по электронной почте, телефону или факсу; посредством технического подключения к инфраструктуре ГосСОПКА:

– в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

– в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

9. Ответственность

9.1. Все работники, осуществляющие защиту ИОД, обрабатываемую в ИС, обязаны ознакомиться с данным Регламентом под подпись.

9.2. Работники несут персональную ответственность за выполнение требований настоящего Регламента.

10. Срок действия и порядок внесения изменений

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

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

10.3. Изменения и дополнения в настоящий Регламент вносятся приказом ректора Учреждения.

Приложение №1
к Регламенту реагирования на
инциденты информационной
безопасности в
информационных системах

Форма
журнала учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки информации в информационных системах

Уч. № _____

Начат: "___" _____ 20__г.

Окончен: "___" _____ 20__г.

На _____ листах

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО ответственного за защиту информации, подпись	ФИО администратора информационной системы, подпись	Примечание
1	2	3	4	5	6