Приложение № 4
к приказу ГАПОУ МИК
от «___»_____20___ года №_____

УТВЕРЖДАЮ
Директор ГАПОУ МИК
И.В.Горшкова
«___»_____2021г.

Положение
о реагировании на инциденты информационной безопасности
в ГАПОУ МИК

Термины, определения и сокращения.

АРМ	–	автоматизированное рабочее место.
АСЭД	–	автоматизированная система электронного документооборота Правительства Оренбургской области.
Актив	–	устройства и/или данные, являющиеся объектами защиты в информационной системе. Включает в себя как сами данные, так и все инфраструктурное оборудование и программное обеспечение.
ГРИИБ	–	группа реагирования на инциденты информационной безопасности, сформированная для обработки инцидентов ИБ во время их жизненного цикла.
ЕИТКС	–	единая информационно-телекоммуникационная сеть правительства Оренбургской области в соответствии положением о ЕИТКС утвержденным постановлением Правительства Оренбургской области от 09.02.2017 № 94-п.
ИБ	–	информационная безопасность – сохранение конфиденциальности, целостности и доступности информации
ИС	–	информационная система.
Образовательное учреждение	–	ГАПОУ МИК.
ОС	–	операционная система.
ОИВ	–	орган исполнительной власти Оренбургской области.
ОМСУ	–	орган местного самоуправления Оренбургской области.
ПО	–	программное обеспечение.
СВТ	–	средства вычислительной техники.
СЗИ	–	средства защиты информации.
СОВ	–	система обнаружения вторжений.
САВЗ	–	система антивирусной защиты.
Свойства ИБ	–	группа свойств, включающая в себя конфиденциальность, целостность и доступность.
Событие ИБ	–	любое идентифицированное явление в системе или сети, указывающего на возможное нарушение установленных свойств информационной безопасности данных, отказ защитных мер или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.
Инцидент ИБ	–	событие, являющееся следствием одного или нескольких событий ИБ, имеющих значительную вероятность или подтверждение нарушения

		установленных свойств информационной безопасности данных, или негативное влияние на состояние системы, сервиса или сети, или создания угрозы информационной безопасности.
Управление инцидентами ИБ	–	деятельность, направленная на своевременное обнаружение инцидентов ИБ и оперативное реагирование на них, минимизацию и (или) ликвидацию негативных последствий от инцидентов ИБ для Министерства, ЕИТКС, ОИВ, ОМСУ и подведомственных им учреждений.
Триггер	–	событие ИБ, являющееся сигналом для инициации процедуры поиска инцидента ИБ в ходе текущего, либо последующих взаимосвязанных событий.
DHCP	–	(Dynamic Host Configuration Protocol) – протокол динамической конфигурации хоста (узла)
DNS	–	(Domain Name System) – система доменных имен
NTP	–	(Network Time Protocol) – сетевой протокол времени
SIEM	–	(Security information and event management) – система управления ИБ и контроля защищенности, обеспечивающая анализ в реальном времени событий ИБ, исходящих от сетевых устройств, приложений, СОВ, САВЗ, и позволяющая реагировать на них до наступления существенного ущерба.

I. Общие положения.

1. Настоящее Положение разработано в целях:

минимизации ущерба от инцидентов ИБ;

предотвращения и (или) снижения негативного влияния инцидентов ИБ на работу образовательного учреждения;

создания условий, способствующих своевременному обнаружению и оперативному реагированию на инциденты информационной безопасности;

обеспечения возможности оперативного внесения изменений и доработок в системы обеспечения информационной безопасности образовательного учреждения;

повышения уровня осведомленности и эффективности работы сотрудников образовательного учреждения в части обеспечения информационной безопасности.

2. Настоящее Положение определяет:

структуру группы реагирования на инциденты информационной безопасности, права и обязанности её участников,

методику обнаружения событий информационной безопасности,

методику формирования инцидентов информационной безопасности,

порядок реагирования на инциденты ИБ.

3. Настоящее Положение разработано в соответствии с:

Федеральным законом от 27.07.2006 № 149–ФЗ «Об информации, информационных технологиях и о защите информации»,

Федеральным законом от 27.07.2006 № 152–ФЗ «О персональных данных»,

Постановлением Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»,

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

4. Требования настоящего Положения являются неотъемлемой частью комплекса мер, направленного на обеспечение безопасности и защиты информации, и распространяются на всех сотрудников образовательного учреждения.

II. Группа реагирования на инциденты информационной безопасности.

5. Состав и роли участников ГРИИБ утверждаются приказом руководителя образовательного учреждения.

Сотрудники с функциональными ролями «Куратор» и «Секретарь» (в соответствии с п. 6 настоящего Положения) назначаются исключительно из

числа сотрудников, курирующих направление информационной безопасности образовательного учреждения.

6. В рамках ГРИИБ определены следующие функциональные роли:

Куратор;

Руководитель;

Секретарь;

Аналитик;

Оператор.

Роль Куратора и роль Руководителя могут быть совмещены. Не допускается совмещение роли Руководитель/Куратор с ролью Оператор/Аналитик. Роль Секретаря, Оператора и Аналитика может выполнять один работник при небольшой численности специалистов по информационной безопасности.

Подробное описание функциональной ролевой модели ГРИИБ приведено в Приложении № 2 к Положению.

7. Правила распространение информации.

Положением определены следующие правила распространение информации о событиях и инцидентах ИБ:

информация об инцидентах ИБ и событиях ИБ является общей для всех участников ГРИИБ и может свободно распространяться между ними;

информация об инцидентах и событиях ИБ может распространяться за пределы ГРИИБ только сотрудниками, имеющими роли «Куратор» и «Руководитель» (только по согласованию с куратором ГРИИБ);

участники ГРИИБ не вправе разглашать сведения, полученные при расследовании инцидента ИБ, за исключением утвержденной куратором или руководителем информации об инциденте ИБ для сотрудников образовательного учреждения, ОИВ, ОМСУ и подведомственных им учреждений. Распространение подобной информации за пределы ГРИИБ является инцидентом ИБ и влечет за собой меры юридической ответственности в отношении нарушителя в соответствии с разделом VI Положения.

III. События ИБ.

8. Классификация событий ИБ.

Каждое событие ИБ в ИС считается триггером. Все события разделяются по источнику и категории для классификации и дальнейшей приоритизации обработки.

8.1. Источники событий ИБ:

источники физического (материального) характера (физические (материальные) носители конфиденциальной информации, человеческий фактор, климатический режим помещений и др.);

сетевое оборудование;

web-приложения;

сервисы (DNS, DHCP, NTP, и др.);

ОС;

СОВ;
САВЗ;
SIEM (генерирует потенциальные инциденты ИБ).

8.2. Категории событий ИБ.

Для событий ИБ определен следующий набор категорий:
атака;
администрирование;
авторизация / завершение сеанса пользователя;
аномальная активность;
воздействие вредоносного кода;
запуск средств анализа уязвимостей;
изменение прав доступа;
изменение состава / конфигурации;
отключение и / или перезагрузка;
обновление;
приостановка работы;
сбой в работе.

Для источника «SIEM» любой сгенерированный потенциальный инцидент ИБ подлежит обработке Аналитиком ГРИИБ.

8.3. Типовые события.

Перечень типовых событий ИБ приведен в Приложении № 3 к Положению.

9. Приоритизация.

Каждому событию ИБ в зависимости от источника и категории присваивается уровень критичности от 0 до 3. Приоритет в обработке должен отдаваться событиям с большим уровнем критичности.

Модель приоритизации событий ИБ.

Источник События ИБ / Категория события ИБ	Источники физического (материального) характера	сетевое оборудование	web-приложения и сервисы	ОС	СОВ	САВЗ	SIEM
атака	1	2	3	2	3	3	3
администрирование	1	1	1	1	2	1	2
авторизация / завершение сеанса пользователя	0	2	1	1	1	1	1
аномальная активность	1	2	3	2	3	3	3
воздействие вредоносного кода	0	2	3	3	3	3	3
запуск средств анализа уязвимостей	0	2	2	1	2	1	3

изменение прав доступа	1	3	1	2	3	2	3
изменение состава / конфигурации	2	2	1	1	3	1	3
отключение и / или перезагрузка	1	3	3	1	3	2	3
обновление	1	2	2	1	3	1	3
приостановка работы	2	3	3	1	3	2	3
сбой в работе	2	3	3	2	3	3	3

IV. Реагирование на инциденты ИБ.

10. В целях реализации реагирования выделяются две основные стадии жизненного цикла инцидента ИБ:

реагирование на инцидент ИБ;

расследование инцидента ИБ.

11. Реагирование на инцидент ИБ.

Этапы реагирования на инцидент ИБ:

обнаружение;

анализ;

регистрация;

сдерживание;

восстановление.

11.1. Этап 1 – Обнаружение.

На данном этапе осуществляется сбор информации о событиях ИБ автоматическим, ручным или автоматизированным способом из источников, указанных в пункте 8.1 Положения, с учетом правил приоритизации, установленных п. 9 Положения.

Порядок действий на этапе обнаружения:

ЭТАП	ОТВЕТСТВЕННЫЕ СОТРУДНИКИ
	Оператор ГРИИБ
1 – Обнаружение	(1) Сбор информации о событиях в ИС.
	(2) Выявление событий ИБ.
	(3) Передача выявленных событий Аналитику.

11.2. Этап 2 – Анализ.

Данный этап разделяется на следующие подэтапы:

сопоставление выявленного события ИБ с другими событиями информационной системы, выявление наступивших или потенциально возможных негативных последствий (если негативные последствия не зафиксированы до момента фиксации инцидента, то это не означает, что негативные последствия не наступят позже;

фиксация индикаторов компрометации (индикаторами компрометации будут являться все следы выявленного события ИБ;

проверка выявленного события ИБ на предмет «ложного срабатывания» СОВ (в случае если негативные последствия не подтвердились, но событие ИБ было зарегистрировано СОВ, принимается решение о присвоения статуса «ложного срабатывания» и вносятся соответствующие корректировки в правила сопоставления, для исключения появления подобного события ИБ в автоматическом режиме).

Потенциальные инциденты ИБ, сгенерированные SIEM в автоматическом режиме подлежат обработке Аналитиком ГРИИБ.

Порядок действий на этапе анализа:

ЭТАП	ОТВЕТСТВЕННЫЕ СОТРУДНИКИ
	Аналитик ГРИИБ
2 – Анализ	(1) Поиск и сопоставление события(ий) ИБ с другими событиями Активов.
	(2) Выявление наступивших или потенциально возможных негативных последствий для Актива(ов).
	(3) Фиксация индикаторов компрометации.
	(4) Проверка выявленного события ИБ на предмет «ложного срабатывания» СОВ, САВЗ, SIEM.
	(5) Если событие(я) ИБ имеет(ют) признаки инцидента ИБ – доклад Руководителю ГРИИБ.

11.3. Этап 3 – Регистрация.

На данном этапе принимается решение о регистрации события ИБ в качестве инцидента ИБ в электронном виде, в формате карточки Инцидента ИБ, в соответствии с Приложением № 1 к Положению.

Для каждого инцидента устанавливается уровень критичности и соответствующие ему критерии реакции:

Критерий инцидента	Уровень критичности инцидента				
	Незначимый	Низкий	Средний	Высокий	Критический
Видимый ущерб активу	Нет	Нет	Нет	Нет	Высокий
Потенциальный ущерб активу	Низкий	Низкий	Средний	Высокий	Высокий
Влияние на информационные процессы в момент инцидента	Нет	Нет	Нет	Да	Да
Возможность спрогнозировать величины ущерба	Да	Да	Да	Да	Нет
Критерии реакции	Уровень критичности инцидента				
	Незначимый	Низкий	Средний	Высокий	Критический
Начало реагирования с момента обнаружения	По мере возможности	1 ч	30 мин.	15 мин.	Немедленно
Принятие компенсирующих мер	По мере возможности	48 ч.	12 часов.	4 ч.	до 1 ч.
Работа с инцидентом, внерабочее время/выходные дни	Нет	Нет	Да/Нет	Да	Да

Порядок действий на этапе регистрации:

ЭТАП	ОТВЕТСТВЕННЫЕ СОТРУДНИКИ	Время
З – Регистрация	Куратор ГРИИБ	
	(1) Информирование руководства образовательного учреждения о выявленном инциденте ИБ.	
	(2) Согласование способа оповещения сотрудников образовательного учреждения об инциденте ИБ.	
	Руководитель ГРИИБ	
	(1) Принятие решения о присвоении событию ИБ статуса «Инцидента ИБ».	
	(2) Присвоение «Уровня критичности» инциденту ИБ.	
	(3) Назначение ответственного Аналитика ГРИИБ.	
	(4) Доклад о выявленном инциденте ИБ Куратору ГРИИБ.	
	Секретарь ГРИИБ	
	(1) Оповещение сотрудников образовательного учреждения об инциденте ИБ по согласованию с Куратором ГРИИБ.	
	(2) Подготовка отчета об инциденте ИБ, доклад Куратору ГРИИБ.	
	Аналитик ГРИИБ	
	(1) Формирование карточки инцидента в электронном виде, по распоряжению Руководителя (в соответствии с Приложением №1).	

11.4. Этап 4 – Сдерживание.

На данном этапе членами ГРИИБ осуществляется идентификация всех скомпрометированных Активов, а также перенастройка систем безопасности таким образом, чтобы избежать потенциальных негативных последствий выявленного инцидента ИБ. По возможности, на данном этапе следует временно изолировать от сети скомпрометированные Активы. Вопрос применения компенсирующих мер рассматривается в соответствии с уровнем критичности инцидента, определенном на этапе регистрации.

Ответственным сотрудником является руководитель структурного подразделения образовательного учреждения, ответственного за Актив, в котором произошел инцидент ИБ.

Порядок действий на этапе сдерживания:

ЭТАП	ОТВЕТСТВЕННЫЕ СОТРУДНИКИ	Время реакции
4 – Сдерживание	Куратор ГРИИБ	
	(1) Контроль отправки информации об инциденте ИБ в национальный координационный центр по инцидентам ИБ.	до 12 ч
	Руководитель ГРИИБ	
	(1) Принятие решения о возможности применения компенсирующих мер к скомпрометированным компонентам ИС, доведение данного решения до Аналитика.	По уровню критичности: до 48 ч (низкий); до 12 ч (средний); до 4 ч (высокий); немедленно (критический)
	(2) Принятие решения об исключении из работы ИС скомпрометированных компонентов и их изоляции от сети, доведение данного решения до Аналитика.	до 20 мин.
	(3) Согласование рекомендаций и(или) требований по устранению выявленного инцидента ИБ и его последствий (потенциально возможных последствий), предложенных Аналитиком.	до 20 мин.
	Секретарь ГРИИБ	
	(1) Информирование руководителя подразделения, отвечающего за работу скомпрометированной ИС, об инциденте ИБ.	до 15 мин.

ЭТАП	ОТВЕТСТВЕННЫЕ СОТРУДНИКИ	Время реакции
	(2) Подготовка отчета о реагировании на инциденте ИБ, доклад Куратору о результатах реагирования.	до 12 ч
	Аналитик ГРИИБ	
	(1) Выявление компонентов ИС, скомпрометированных в рамках выявленного инцидента.	до 40 мин.
	(2) Формирование рекомендаций и(или) требований по устранению выявленного инцидента ИБ и его последствий (потенциально возможных последствий), согласование их с Руководителем.	до 1,5 ч
	(3) Доведение до ответственного сотрудника согласованных Руководителем рекомендаций и(или) требований по устранению выявленного инцидента ИБ и его последствий (потенциально воозможных последствий) в свободной форме по наиболее скоростному каналу передачи данных, с указанием уровня критичности и срока исполнения.	до 15 мин.
	(4) Оформление служебной записки в АСЭД на Ответственного сотрудника с согласованными рекомендациями (требованиями), запросом информации о сроке их исполнения, последствиях и полученном ущербе от инцидента ИБ, дополнительных сведений, необходимых для заполнения карточки инцидента ИБ. Данный пункт обязателен только для инцидентов ИБ с уровнем критичности «Высокий» и «Критический», в остальных случаях – на усмотрение Аналитика, по согласованию с Руководителем.	до 2 ч.
	Ответственный сотрудник	
	(1) Исполнение требований по устранению выявленного инцидента ИБ и его последствий (потенциально возможных последствий), поступивших от Аналитика в рабочем порядке, при	По уровню критичности: до 48 ч (низкий); до 12 ч (средний); до 4 ч (высокий);

ЭТАП	ОТВЕТСТВЕННЫЕ СОТРУДНИКИ	Время реакции
	частичной или полной невозможности исполнения указанных в служебной записке рекомендаций и (или) требований – направление мотивированного отказа.	немедленно (критический)
	(2) Оформление ответа на служебную записку Аналитика в АСЭД.	до 2 ч

Общее время реакции: не более 48 ч с момента принятия Руководителем решения о присвоении событию статуса инцидента ИБ.

11.5. Этап 5 – Восстановление.

Цель данного этапа – приведение Актива в состояние, в котором он находился до возникновения инцидента ИБ.

Порядок действий на этапе восстановления:

ЭТАП	ОТВЕТСТВЕННЫЕ СОТРУДНИКИ	Время реакции
5 – Восстановление	Куратор ГРИИБ	
	(1) Принятие решения о необходимости расследования выявленного инцидента ИБ.	до 12 ч
	Руководитель ГРИИБ	
	(1) Принятие решения о закрытии Инцидента ИБ.	
	(2) Контроль возвращения ИС к функционированию в штатном режиме, доклад Куратору по результатам.	до 24 ч
	(3) Подготовка по результатам выявленных инцидентов ИБ предложений, касающихся: внесения изменений в системы ИБ; внесения изменений в процессы менеджмента инцидентов ИБ; внесения изменений в регламенты реагирования на инциденты ИБ; внесения изменений во внутренние нормативные документы.	до 24 ч
	Аналитик ГРИИБ	
	(1) Контроль за возвращением ИС к функционированию в штатном режиме, доклад Руководителю о результатах проведенных мероприятий.	до 24 ч
	Ответственный сотрудник	
	(1) Контроль за возвращением ИС к функционированию в штатном режиме,	до 24 ч

ЭТАП	ОТВЕТСТВЕННЫЕ СОТРУДНИКИ	Время реакции
	доклад Руководителю о результатах проведенных мероприятий.	

12. Расследование инцидента ИБ.

Решение о необходимости проведения расследования принимается Куратором ГРИИБ исходя из уровня критичности инцидента и нанесенного ущерба. Для инцидентов ИБ с уровнем критичности «Высокий» и «Критический» расследование проводится в обязательном порядке. Для проведения расследования Куратором ГРИИБ назначаются ответственные, из числа членов ГРИИБ.

В рамках расследования инцидента ИБ требуется определить:

начальный вектор возникновения инцидента ИБ (пример: внешнее целенаправленное воздействие, внутренний нарушитель и т.д.);

причины возникновения инцидента ИБ (уязвимость, воздействие вредоносного кода, атака и т.д.);

пострадавшие активы, размеры ущерба;

если имела место атака на Актив, то была ли она завершена (была ли атакующими достигнута их цель);

временные рамки инцидента ИБ.

По результатам расследования инцидента ИБ ответственным членом ГРИИБ на имя Куратора формируется служебная записка в АСЭД.

V. Контроль.

13. Контроль за выполнением требований настоящего Положения осуществляет заместитель директора по безопасности образовательного процесса.

VI. Ответственность.

14. Требования Положения обязательны для исполнения сотрудниками образовательного учреждения, входящими в состав ГРИИБ.

15. Сотрудники образовательного учреждения несут ответственность за нарушение требований Положения в соответствии с законодательством Российской Федерации и локальными актами образовательного учреждения .

Приложение № 1
к Положению

Перечень сведений, содержащихся в карточке инцидента ИБ

Карточка инцидента оформляется и хранится в электронном виде, содержит следующие сведения и должна иметь следующую структуру:

1. Идентификационный номер инцидента ИБ.
2. Информация о сообщающем лице:

а) фамилия;

б) имя;

в) отчество;

г) адрес электронной почты;

д) контактный телефон;

е) дополнительная информация по усмотрению сообщающего.

3. Описание события(ий) ИБ (данный раздел может быть не один, поскольку инцидент могут вызвать совокупность событий ИБ):

а) детали события;

б) дата и время возникновения события;

в) дата и время обнаружения события;

г) дата и время сообщения о событии Руководителю ГРИИБ;

д) источник события (Актив, SIEM, сотрудник, внешний источник и т.д.);

е) любая дополнительная информация, которая может быть полезной при дальнейшем расследовании инцидента ИБ (файлы протоколирования, отчеты, скриншоты, изображения, файлы конфигураций и т.д.);

ж) закончилось ли событие на момент обнаружения (Да/Нет);

з) продолжительность события (суммарное время подробно, если были зафиксированы временные интервалы)

4. Информация об инциденте ИБ:

а) тип инцидента ИБ (действительный, попытка, подозрение);

б) тип угрозы Активу (компрометация, нарушения целостности, нарушение доступности, нарушение отказоустойчивости, утрата);

в) тип воздействия на Актив (намеренный, случайный, ошибка):

если «Намеренный» – выбрать из следующих вариантов:

хищение;

мошенничество;

сознательное причинение физического ущерба;

вредоносная программа;

хакерство/логическое проникновение;

неправильное использование ресурсов;

другое (описать*)*;

если «Случайный» – выбрать из следующих вариантов:

отказ оборудования;

отказ ПО;

отказ связи;

пожар, наводнение;

отказ электропитания;

другое природное явление (определить);

если «Ошибка» выбрать – из следующих вариантов:

ошибка ПО;

ошибка оборудования;

ошибка пользователя;

ошибка администратора;

ошибка проектирования (не выполнение функций при расчетной нагрузке);

другой вариант (описать);

г) пораженные Активы:

информация/данные (описать);

оборудование(описать);

программное обеспечение(описать);

средства связи(описать);

документация (описать).

5. Информация о разрешении инцидента ИБ:

а) ФИО Аналитика ГРИИБ, ответственного за разрешение инцидента;

б) ФИО ответственного(ых) сотрудников (администраторы Активов, с которыми произошел инцидент);

в) дата и время начала реакции Аналитика ГРИИБ на инцидент;

г) дата и время окончания реакции Аналитика ГРИИБ на инцидент;

д) дата и время направления рекомендаций/требований ответственным сотрудникам;

е) содержание рекомендаций/требований, направленных ответственным сотрудникам;

ж) дата и время исполнения рекомендаций/требований ответственными сотрудниками;

з) дополнительная информация (невозможность исполнить рекомендации/требования, любая дополнительная информация о принятых мерах в рамках реакции на инцидент);

и) дата и время завершения всех работ по инциденту инцидента.

6. Информация о расследовании инцидента.

Информация о расследовании инцидента ИБ должна быть максимально полной и включать все материалы, обосновывающие выводы о причинах возникновения инцидента.

Информация о расследовании инцидента ИБ должна содержать:

а) ФИО участников расследования (от кого, какая, когда была получена информация о событиях ИБ, способствовавших возникновению инцидента);

б) выводы о причинах возникновения инцидента ИБ;

в) принятые меры для исключение подобных инцидентов в будущем; дополнительная информация.

Приложение № 2
к Положению

Функциональная ролевая модель

Роль в ГРИИБ	Задача в рамках ГРИИБ	Функциональные обязанности	Подчиненность	Совмещение	Ответственность
1	2	3	4	5	6
Куратор	общее руководство деятельность ю ГРИИБ, контроль своевременности и достаточности процессов реагирования на инциденты ИБ в образовательном учреждении	1. Принятие управленческих решений по результатам реагирования на инциденты ИБ. 2. Информирование руководства образовательного учреждения об обнаруженных инцидентах ИБ и результатах реагирования на них. 3. Привлечение сотрудников необходимыми компетенциями в рамках ГРИИБ для реагирования на инциденты ИБ. 4. Оповещение сотрудников образовательного учреэждения об инциденте ИБ в соответствии с установленными регламентами. 5. Принятие решений о необходимости проведения расследований по инцидентам ИБ. 6. Принятие решений о необходимости привлечения к расследованиям инцидентов ИБ правоохранительных органов, представителей регуляторов в области ИБ, сторонних организаций.	Руководитель образовательног о учреждения	совмещение с другими ролями не допускается	персональная ответственность за: выполнение возложенных функциональных обязанностей; общую эффективность работы ГРИИБ.

1	2	3	4	5	6
		7. Информирование национального координационного центра об инцидентах ИБ, в случае если передача информации о них в центр ГосСОПКА не возможна в полуавтоматическом режиме.			
Руководитель	оперативное руководство деятельностью ГРИИБ	1. Организаци реагирования на инциденты ИБ в ГРИИБ. 2. Назначение ответственного исполнителя ГРИИБ для реагирования на инцидент ИБ. 3. Координирование деятельности членов ГРИИБ в рамках реагирования на инцидент ИБ. 4. Контроль за соблюдением членами ГРИИБ требований регламентирующих документов. 5. Принятие решений о завершении всех работ по инциденту ИБ. 6. Координирование и контроль оформления инцидента ИБ. 7. Подготовка по результатам выявленных инцидентов ИБ предложений, касающихся: внесения изменений в системы ИБ, внесения изменений в процессы управления инцидентами ИБ, внесения изменений в регламенты реагирования на инциденты ИБ, внесения изменений в локальные акты. 8. Внесение предложений о взаимодействии в рамках расследования инцидента с правоохранительными органами и	Куратор ГРИИБ	возможно совмещение с ролью «Аналитик»	Персональная ответственность за: выполнение возложенных функциональных обязанностей; оперативное принятие решений и выработку компенсирующих мер защиты.

1	2	3	4	5	6
		сторонними организациями.			
Секретарь	сбор и анализ информации о событиях и инцидентах ИБ, формирование аналитических отчетов.	1. Сбор и обобщение сведений о событиях и инцидентах ИБ (в том числе событиях ИБ, ошибочно признанных инцидентами ИБ). 2. Подготовка отчетов о зафиксированных инцидентах ИБ. 3. Подготовка отчетов о результатах реагирования на инциденты ИБ. 4. Подготовка отчетов о результатах расследования инцидентов ИБ. 5. Оповещение сотрудников образовательного учреждения об инцидентах ИБ по поручению Куратора и в соответствии с установленными регламентами	Куратор ГРИИБ	возможно совмещение с ролью «Аналитик»	Персональная ответственность за: выполнение возложенных функциональных обязанностей; сбор и систематизацию данных об инцидентах и событиях ИБ, достоверность предоставляемых аналитических отчетов.
Аналитик	Обработка информации обнаруженных и зарегистрированных инцидентах ИБ	1. Проведение вторичной оценки инцидентов ИБ с целью подтверждения правильности оценки события ИБ Оператором. 2. Проведение мероприятий по реагированию на инцидент ИБ. 3. Проведение расследования инцидента ИБ, сбор и фиксация информации об инциденте. 4. Взаимодействие с сотрудниками, имеющими роли «Руководитель» и «Оператор» по вопросам реагирования на инцидент ИБ. 5. Взаимодействие с сотрудником, имеющим	Руководитель ГРИИБ	возможно совмещение с ролью «Оператор»	Персональная ответственность за: выполнение возложенных функциональных обязанностей; оперативное реагирование на поступающие события ИБ.

1	2	3	4	5	6
		роль «Секретарь» по вопросам предоставления информации об инциденте.			
Оператор	обнаружение и регистрация событий и инцидентов ИБ, первичный сбор информации о них	1. Мониторинг событий ИБ. 2. Сбор информации о событиях ИБ и (или) любых подозрительных событиях, имеющих отношение к ИБ. 3. Проведение первичной оценки выявленных событий ИБ на предмет их принадлежности к категории инцидентов ИБ. 4. Регистрация событий ИБ. 5. Регистрация инцидентов ИБ и незамедлительное информирование сотрудника, имеющего роль «Аналитик» о них.	Аналитик ГРИИБ	совмещение с другими ролями не допускается	Персональная ответственность за: выполнение возложенных функциональных обязанностей; оперативное реагирование на поступающие события ИБ.

Приложение № 3
к Положению

Типовые события ИБ

Источник событий ИБ	Описание события
Источники физического (материального) характера	– физический доступ к АРМ сотрудников или телекоммуникационному оборудованию; – изменение параметров настроек СВТ и (или) телекоммуникационного оборудования, – сбои и отказы в работе СВТ и (или) телекоммуникационного оборудования, – сбои и отказы в работе СЗИ, – отказы в работе сетей передачи данных. – физическое воздействие на СВТ, СЗИ, телекоммуникационное оборудование и сети передачи данных, – изменение климатического режима помещений, в которых расположены СВТ и (или) телекоммуникационное оборудование, – изменение параметров функционирования сетей передачи данных, – вынос СВТ за пределы контролируемых помещений, – передача СВТ во внешние организации, – события, формируемые охранной сигнализацией, – события, формируемые системой контроля и управления доступом, – физический доступ к компонентам охранной сигнализации, – физический доступ к компонентам системы контроля и управления доступом.
Сетевое оборудование	– изменение настроек, – внесение изменений в ПО, – аномальная сетевая активность, – аутентификация и завершение сеанса работы сотрудника, – обнаружение вредоносного кода или следов его воздействия,

Источник событий ИБ	Описание события
	– изменение топологии вычислительной сети, – подключение оборудования к вычислительной сети, – сбои в работе ПО, – обновление ПО, – выполнение технического обслуживания, – отключение и (или) перезагрузка оборудования, – обнаружение атак вида «отказ в обслуживании», – смена и (или) компрометация аутентификационных данных, – сбои и отказы в работе СЗИ, – изменение параметров работы и (или) конфигурации СЗИ, – применение средств анализа уязвимостей / топологии сети.
Web–приложения и сервисы	– атаки («фишинговые», сетевые и т.д.), – авторизация и (или) завершение сеанса работы сотрудника, – изменение состава и (или) конфигурации ПО, – обнаружение вредоносного кода или следов его воздействия, – установка удаленных соединений, – сбои и отказы в обслуживании сетевых приложений и сервисов, – выполнение операций, связанных с администрированием сетевых приложений и сервисов, – обнаружение нетипичных (аномальных) запросов, – отключение / перезагрузка или остановка в работе сетевых приложений и сервисов, – выполнение операций со списками рассылки и (или) адресными книгами, – изменение прав доступа сотрудников, – применение средств анализа уязвимостей, – смена и (или) компрометация аутентификационных данных сотрудников, – сбои и отказы в работе СЗИ, – изменение параметров работы и (или) конфигурации СЗИ, – переадресация сообщений, в том числе электронной почты, – выполнение операций со средствами криптографической защиты информации и ключевой информацией.
ОС	– аутентификация и завершение сеанса работы,

Источник событий ИБ	Описание события
	– изменение состава и (или) конфигурации ПО, – запуск, остановка и (или) отключение/перезагрузка ПО, – обнаружение вредоносного кода или следов его воздействия, – обнаружение нетипичных (аномальных) запросов с использованием прикладного ПО, – сбои и отказы в работе СЗИ, – изменение параметров работы и (или) конфигурации СЗИ, – применение средств анализа уязвимостей, – выполнение операций со средствами криптографической защиты информации и ключевой информацией.