Приложение 8

УТВЕРЖДЕНО
приказом ГАОУ ВО МИОО
от 25.10.2017 № 406/ОД

ПОЛИТИКА МОНИТОРИНГА СОБЫТИЙ И УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГОСУДАРСТВЕННОМ АВТОНОМНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ВЫСШЕГО ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ «МОСКОВСКИЙ ИНСТИТУТ ОТКРЫТОГО ОБРАЗОВАНИЯ»

Москва, 2017 г.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящая Политика мониторинга событий и управления инцидентами информационной безопасности в Государственном автономном образовательном учреждении высшего образования города Москвы «Московский институт открытого образования» (далее – Политика) является внутренним нормативным документом Государственного автономного образовательного учреждения высшего образования города Москвы «Московский институт открытого образования» (далее – Институт) и не подлежит представлению другим сторонам без согласования с ректором Института.

1.2 Настоящая Политика определяет требования к процессам мониторинга событий ИБ и управления инцидентами информационной безопасности в Институте, распространяется на все информационные системы (далее – ИС) Института и их компоненты и обязательна для выполнения всеми работниками Института.

1.3 Управление инцидентами информационной безопасности должно проводиться в соответствии с требованиями законодательства Российской Федерации и настоящей Политики. Своевременное информирование об инцидентах информационной безопасности и содействие лицам, ответственным за управление инцидентами информационной безопасности, должно являться обязательной составляющей выполнения работниками Института их должностных обязанностей.

2. ОБЩИЕ ПОЛОЖЕНИЯ

Процесс управления инцидентом ИБ включает:

- сбор и хранение событий ИБ в ИС,
- обнаружение инцидента ИБ,
- проверку достоверности информации об инциденте ИБ,
- классификацию инцидента ИБ,
- уведомление об инциденте ИБ,
- регистрацию и протоколирование инцидента ИБ,
- устранение инцидента ИБ,
- расследование инцидента ИБ,
- устранение последствий инцидента ИБ.

Исполнение процесса управления инцидентами ИБ должно быть обеспечено в круглосуточном режиме в рабочие, выходные и праздничные дни.

3. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе использованы следующие термины, определения и сокращения:

Актив – все, что в сфере деятельности Института, связанной с созданием, преобразованием и потреблением информации, представляет для нее интерес и имеет ценность. Основными характеристиками активов, рассматриваемых в рамках оценки рисков информационной безопасности, являются конфиденциальность, целостность и доступность.

К активам могут относиться, но не ограничиваясь, следующие сущности:

– информационные активы (в электронном виде и на материальных носителях), создаваемые, получаемые, передаваемые, хранимые и обрабатываемые с использованием автоматизированных и телекоммуникационных систем и сервисов;

– программные активы – прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты;

– персонал, осуществляющий обработку информации с использованием автоматизированных информационных систем;

– сервисы – вычислительные и коммуникационные сервисы, предоставляемые с использованием автоматизированных информационных систем;

– физические активы – компьютеры и коммуникационное оборудование, магнитные, оптические и иные носители данных (ленты, диски и т.д.), используемые для обработки, хранения или передачи информационных активов, другое техническое оборудование (блоки питания, кондиционеры и т.д.), мебель, помещения, здания.

Владелец информационной системы – работник или руководитель структурного подразделения Института, в интересах которого данная ИС создана, или третье лицо (в случае использования внешней ИС). Владелец информационной системы является частным случаем владельца информационного ресурса.

ИБ – информационная безопасность.

Институт – Государственное автономное образовательное учреждение высшего образования города Москвы «Московский институт открытого образования».

Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов, а также иная информация, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах), а также информационные системы и их элементы, служащие для обработки документов (информации).

Инцидент информационной безопасности (инцидент ИБ) – событие и/или серия событий, которые привели, приводят или могут привести с высокой долей вероятности к нарушению бизнес процессов и реализации угроз информационной безопасности.

Информационная система (ИС) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Офицер ИБ – работник Института, назначенный приказом ректора Института на роль ответственного за обеспечение информационной безопасности в Институте, в том числе безопасности персональных данных.

4. МОНИТОРИНГ СОБЫТИЙ ИБ

4.1. Под мониторингом событий ИБ понимается процесс просмотра и анализа журналов зарегистрированных событий ИС Института, проводимый с целью выявления инцидентов ИБ и их регистрации.

4.2. Мониторинг событий ИБ осуществляется непрерывно, с использованием системы управления событиями ИБ (в случае ее применения в Институте), а также

через консоли централизованного управления соответствующих систем защиты информации, в том числе:

– систем антивирусной защиты;

– систем обнаружения вторжения;

– межсетевых экранов и маршрутизаторов;

– систем предотвращения утечек конфиденциальной информации;

– систем аудита операционных систем, систем управления базами данных, систем виртуализации, прикладного ПО;

– других компонентов ИС.

4.3. Мониторинг событий осуществляют специалисты управления информатизации (в отношении ИС которые они поддерживают) в ручном и/или автоматизированном режиме:

– в ручном режиме: специалисты управления информатизации не реже одного раза в рабочий день просматривают и анализируют события, зарегистрированные системами Института, на предмет обнаружения отклонений от нормального режима функционирования систем и выявления инцидентов ИБ. Обо всех выявленных инцидентах специалисты ИТ подразделения незамедлительно информируют офицера ИБ;

– в автоматизированном режиме: журналы регистрации событий всех систем Института анализируются системой управления событиями ИБ на предмет выявления инцидентов ИБ.

4.4. В случае выявления инцидентов ИБ система управления событиями ИБ автоматически направляет офицеру ИБ и специалистам управления информатизации уведомление по электронной почте или sms.

4.5. Ежедневному автоматизированному и/или ручному мониторингу подлежат все события ИБ, зарегистрированные всеми ИС, перечень которых приведен в п. 4.2.

4.6. Журналы регистрации событий должны храниться не менее одного года на сервере системы управления событиями ИБ или непосредственно в информационной системе (в случае если мониторинг событий, регистрируемых данной системой, не осуществляется системой управления событиями ИБ).

5. ПРЕДОТВРАЩЕНИЕ ИНЦИДЕНТОВ ИБ

5.1. В Институте внедрены следующие механизмы их предотвращения инцидентов ИБ:

– утверждены внутренние нормативные документы, определяющие политику Института в области информационной безопасности;

– совершенствуются технические меры по предотвращению Инцидентов ИБ;

– все работники Института (штатные, временные, внештатные) и контрагенты подписывают с Институтом соглашение о конфиденциальности;

– ИС Института разрабатываются и внедряются с учётом внутренних нормативных документов, регламентирующих обеспечение информационной безопасности;

– критичные события ИБ регистрируются, проводится расследование и выработка мер по оптимизации рисков возникновения данных событий в будущем;

– офицер ИБ проводит работу по повышению осведомлённости сотрудников Института в области ИБ;

– процесс управления инцидентами ИБ непрерывно совершенствуется.

6. ТРЕБОВАНИЯ К ИС

6.1. Все ИС Института должны удовлетворять требованиям Политики ИБ и частных политик ИБ, в частности:

– авторизация в соответствии с Политикой парольной защиты;

– запись в журналы регистрации достаточно подробной информации обо всех событиях ИБ. Перечень необходимой информации согласуется в отношении каждой ИС между владельцем ИС и офицером ИБ;

– возможность автоматизированной передачи журналов регистрации во внешнюю систему сбора информации в реальном времени, либо по расписанию с частотой не ниже одного раза в час (в случае ее использования);

– ИС должны обладать вычислительными ресурсами, достаточными для выполнения данных требований без ущерба основному функционалу. Запас ресурсов должен закладываться при проектировании ИС.

6.2. Доступ к журналам регистрации событий ИБ должен быть предоставлен только тем пользователям ИС, кому он необходим для выполнения должностных обязанностей.

6.3. Системное время всех ИС должно быть синхронизировано с единым источником точного времени.

6.4. При наличии технической возможности для каждого компонента ИС Института должен быть реализован механизм протоколирования следующих событий:

– использование механизмов идентификации и аутентификации;

– неуспешные попытки логического доступа;

– любые действия пользователя ИС с персональными данным (согласно пп.8 п.2 ст.19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»);

– блокировка учетной записи в результате превышения лимита неверных попыток входа;

– любые действия, совершенные с использованием административных полномочий;

– изменение идентификационных данных пользователя, в том числе сброс пароля учетной записи с использованием другой учетной записи;

– создание/удаление учетных записей;

– изменение полномочий пользователей;

– создание/удаление групп пользователей/ролей доступа;

– создание/удаление таблиц в БД;

– изменение настроек парольной защиты;

– изменения настроек синхронизации системного времени;

– изменения конфигурации (создание/изменение/удаление правил, добавление/удаление учетных записей);
– любое изменение (в том числе, отключение) параметров аудита в ИС;
– системные ошибки;
– запуск и остановка сервисов;
– доступ к журналам событий ИБ;
– срабатывание сигнатур системы обнаружения вторжений;
– обнаружение вредоносного ПО;
– события, необходимость протоколирования которых дополнительно определена офицером ИБ.

6.5. Для каждого события должны быть записаны как минимум следующие параметры:
– название ИС или его компонента;
– идентификатор пользователя;
– тип события;
– дата и время;
– успешным или неуспешным было событие;
– источник события (например, ip адрес клиента, название рабочей станции и т.п.);
– идентификатор объекта, на который повлияло событие.

7. ОБНАРУЖЕНИЕ ИНЦИДЕНТОВ ИБ

7.1. Источники информации о событиях ИБ:
– пользователи ИС;
– журналы ИС;
– системы сбора и корреляции событий ИБ (в случае их использования в Институте);
– автоматизированные проверки;
– внутренние и внешние аудиты ИБ.

7.2. Офицер ИБ, получивший информацию о событиях ИБ, обязан проверить их достоверность, после чего принять решение о том, является ли данное событие инцидентом ИБ.

7.3. В случае обнаружения инцидента ИБ запускается процедура реагирования в соответствии с настоящей Политикой.

8. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИБ

8.1. Процедура реагирования на инциденты ИБ включает в себя:
– классификацию инцидента ИБ;
– уведомление уполномоченных лиц;
– регистрацию и протоколирование инцидентов ИБ;
– расследование инцидентов ИБ;
– устранение инцидентов ИБ и их последствий.

9. ПРИОРИТЕТЫ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИБ

9.1. При определении категории инцидента ИБ учитывается настоящее и потенциальное воздействие инцидента ИБ на информационные активы Институте, а также ценность подверженных ему информационных активов.

9.2. Реагирование на инциденты ИБ, первичное расследование с целью проверки достоверности фактов, указывающих на инцидент ИБ, возлагается на офицера ИБ и системных администраторов всех затронутых инцидентом информационных систем.

9.3. Время начала реагирования на инцидент безопасности с момента его обнаружения и уведомления уполномоченных работников определяется, исходя из критичности инцидента ИБ согласно п. 10.2 (Таблица 1).

Таблица 1

Максимальное время начала реагирования на инцидент

Категория инцидента (критичность)	Высокая	Средняя	Низкая	Незначительная
Реагирование	15 мин	30 мин	1 час	2 часа

10. КЛАССИФИКАЦИЯ ИНЦИДЕНТОВ ИБ

10.1. Регулярно повторяющиеся инциденты ИБ (например, обнаружение вредоносного ПО) могут классифицироваться автоматически соответствующим программным обеспечением.

10.2. Инциденты ИБ разделяются на категории в зависимости от ценности информационных активов и/или масштабов затрагиваемых информационных активов Института (Таблица 2).

Таблица 2

Уведомление менеджмента об инцидентах ИБ

	Некритичные активы	Активы средней критичности	Критичные активы
Глобальный инцидент (может привести к последствиям на уровне всего Института)	Инцидент высокой критичности	Инцидент высокой критичности	Инцидент высокой критичности
Инцидент среднего масштаба (может привести к последствием на уровне отдельной системы)	Инцидент низкой критичности	Инцидент средней критичности	Инцидент высокой критичности
Локальные инциденты (последствия на уровне отдельного сервиса)	Инцидент незначительной критичности	Инцидент низкой критичности	Инцидент средней критичности

10.3. Оценка степени критичности инцидентов ИБ осуществляется до их наступления на этапе планирования процедур реагирования на инциденты ИБ.

10.4. Вне зависимости от степени критичности инцидента ИБ запускается процедура реагирования в соответствии с настоящей Политикой.

10.5. В случае, когда процедура реагирования на конкретный инцидент ИБ на момент возникновения инцидента не документирована и степень критичности инцидента ИБ не определена, то степень его критичности определяется офицером ИБ экспертным путем с учётом мнения владельца ИС.

10.6. В случае повторения инцидента ИБ в течение ограниченного отрезка времени возможно повышение степени его критичности. Решение о повышении степени критичности инцидента принимает офицер ИБ, основываясь на результатах расследования инцидента ИБ.

11. УВЕДОМЛЕНИЕ ОБ ИНЦИДЕНТАХ ИБ

11.1. Таблица 3 определяет уведомляемых лиц, время уведомления об инциденте ИБ с момента его обнаружения и проверки достоверности фактов, указывающих на инцидент.

Таблица 3

Уведомление менеджмента об инцидентах ИБ

Категория инцидента (критичность)	Высокая	Средняя	Низкая	Незначительная
Уведомляемые лица	Руководство Института Владелец актива	Руководство Института Владелец актива	Владелец актива**	Владелец актива**
Время на оповещение	15 мин*	15 мин*	30 мин*	В течение рабочего дня

* - время с момента проверки достоверности фактов, указывающих на инцидент;

** - в случае определения необходимости расследования инцидента.

11.2. Офицер ИБ осуществляет уведомление об инцидентах ИБ с использованием корпоративной электронной почты, а для инцидентов высокой и средней критичности также по телефону.

11.3. Офицер ИБ ведет журнал учёта произведенных уведомлений.

12. РЕГИСТРАЦИЯ И ПРОТОКОЛИРОВАНИЕ ИНЦИДЕНТОВ ИБ

12.1. Обязательной регистрации подлежат все инциденты ИБ высокой и средней критичности.

12.2. Информация об обнаруженном инциденте ИБ регистрируется офицером ИБ в соответствии с формой, которую содержит Приложение 1.

12.3. Первичное определение категории инцидента ИБ возлагается на офицера ИБ, ответственного за регистрацию инцидента ИБ.

12.4. На протяжении всего цикла управления инцидентом ИБ осуществляется протоколирование инцидента ИБ и регистрация дополнительных данных.

12.5. Срок хранения данных по инцидентам ИБ не ограничен с целью формирования статистических данных по инцидентам ИБ.

12.6. Доступ к протоколам регистрации и расследования инцидентов ИБ предоставляется только по согласованию офицера ИБ.

13. РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИБ

13.1. Расследованию подлежат все инциденты высокой и средней критичности. Расследование инцидентов других категорий проводится по инициативе руководства Института, офицера ИБ или руководителей затронутых инцидентом подразделений.

13.2. Расследование инцидентов проводится с целью выявления причин возникновения инцидента, разработки корректирующих действий, позволяющих в будущем минимизировать воздействие инцидента и/или избежать его повторения, и проводится после устранения инцидента.

13.3. Расследование инцидентов проводится группой расследования под руководством офицера ИБ, которая формируется из уполномоченных работников заинтересованных подразделений (в зоне ответственности которых произошел инцидент), делегированных руководителями данных подразделений.

13.4. Группа расследования ответственна за сбор возможных документированных материалов расследования (свидетельств инцидента). Собранная информация должна храниться в течение пяти (5) лет.

13.5. В рамках расследования инцидента представители группы расследования имеют право:

– на непосредственный доступ в помещения Института, где произошел инцидент, в том числе к рабочему месту работников, принявших прямое или косвенное участие в инциденте, а также иному аппаратному обеспечению;

– требовать от работников Института представления документов или иной информации, относящейся к расследованию, для ознакомления с ней и приобщения к материалам расследования;

– требовать от работников Института написания объяснительных записок по факту прямого или косвенного участия в инциденте;

– вызывать работников Института для проведения личной беседы по факту прямого или косвенного участия в инциденте.

13.6. В рамках проведения расследования инцидента работники Института, по требованию представителя группы расследования, обязаны предоставить:

– запрашиваемую представителем группы расследования информацию;

– письменные объяснения;

– доступ в помещения Института, в том числе к своему рабочему месту, а также иному аппаратному обеспечению.

13.7. В рамках расследования инцидента представители группы расследования обязаны:

– руководствоваться требованиями законодательства РФ;

– соблюдать права и свободы граждан РФ согласно Конституции РФ;

– принимать все меры, необходимые для объективного проведения расследования;

– обеспечивать сохранность и конфиденциальность материалов, приобщаемых к расследованию инцидента.

13.8. По результатам проведения расследования инцидента группа расследования предоставляет отчет для руководителя, принявшего решение о проведении расследования, а в случае инцидента высокой и средней критичности – для руководства Института.

13.9. В отчете указывается описание инцидента, результаты расследования и рекомендации (корректирующие действия) по снижению риска повторения инцидента или подобных инцидентов.

14. УСТРАНЕНИЕ ИНЦИДЕНТОВ ИБ И ИХ ПОСЛЕДСТВИЙ

14.1. Устранение инцидента ИБ высокой и средней критичности начинается сразу после его обнаружения.

14.2. Устранение инцидента не должно приводить к уничтожению доказательств инцидента ИБ.

14.3. Устранение инцидентов ИБ и их последствий производится в соответствии с Планами реагирования на конкретный тип инцидента ИБ (Приложение 3).

14.4. При отсутствии плана реагирования для конкретного типа инцидента ИБ устранение осуществляется под руководством офицера ИБ. После устранения последствий такого инцидента ИБ офицер ИБ принимает решение о необходимости разработки плана реагирования для данного типа инцидентов ИБ.

14.5. При восстановлении функционирования ИС могут использоваться последние резервные копии данных и настроек систем.

14.6. После завершения расследования инцидента ИБ владельцы ИС совместно с офицером ИБ и специалистами управления информатизации разрабатывают корректирующие действия, позволяющие в будущем минимизировать воздействие инцидента и/или избежать его повторения.

15. ПЛАНЫ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИБ

15.1. Для инцидентов ИБ, способных нанести значительный ущерб критичным активам Института, привести к серьезным потерям, а также для часто повторяющихся инцидентов, офицер ИБ совместно со специалистами управления информатизации должны разрабатывать детальные планы реагирования. Приложение 3 содержит форму плана реагирования.

15.2. Утверждение планов реагирования на инциденты ИБ осуществляется проректором по информационным технологиям.

15.3. Планы реагирования на инциденты ИБ должны содержать:

– последовательность действий по устранению инцидента;

– последовательность действий по уведомлению руководства и заинтересованных сторон;

– последовательность действий по устранению последствий инцидента;

– перечень лиц, ответственных за реагирование.

15.4. Планы реагирования на инциденты должны быть доведены до работников Института, ответственных за реагирование.

15.5. Для оценки эффективности и результативности планов реагирования на инциденты ИБ, каждый из разработанных планов должен проходить ежегодное тестирование.

16. КОНТАКТНАЯ ИНФОРМАЦИЯ

16.1. Контактная информация работников, уведомляемых об инцидентах, указана в памятках (Приложение 2), заполняемых офицером ИБ.

16.2. Руководители подразделений обеспечивают распространение указанной в памятках информации среди работников своих подразделений.

Приложение 1
к Политике мониторинга
событий и управления
инцидентами ИБ

ОТЧЕТ
об инциденте ИБ №__

Информация об Институте

Адрес		
Подразделение		
Информационная система/ Актив (если применимо)		
Информация получена от:	ФИО	
	e-mail	
	Телефон	

Информация об инциденте

Дата и время начала инцидента		Дата и время обнаружения инцидента	

Уведомление об инциденте:

Уведомлены:	Дата, время и способ уведомления:

Как был обнаружен инцидент?

Работником:	ФИО:	
	Должность:	
	Телефон:	
В ходе автоматизированной проверки средством мониторинга:	Проверка:	
	Описание проверки:	
Другое:		

Кратко опишите предпосылки обнаружения инцидента (например, задымление, сообщение клиента (ов) о недоступности сервиса, сбои в работе ИС и т.д.)

Инцидент окончен?
Да ☐ Нет ☐

Укажите тип, успех (реальный/ потенциальный) и намерение (случайный/ намеренный) инцидента:

Тип	Конфиденциальность (разглашение)	Целостность (изменение)	Доступность (отказ или разрушение)
Успех			
Намерение			

Укажите наиболее существенное воздействие инцидента и оцените его (незначительное/ низкое/ среднее/ высокое):

Затруднения в работе Института	
Безопасность работников	
Финансовые потери	
Репутационные (имиджевые) потери	
Разрушение процессов	
Безопасность персональных данных	
Разглашение конфиденциальной информации	
Нарушение требований законодательства и контрактных обязательств	

Перечислите все активы подверженные или компрометированные инцидентом:

Аппаратные средства	
Программные средства	
Сервисы	
Каналы и средства связи	
Персонал	
Помещения	
Информация в электронном виде	
Информация в бумажном виде	
Иные	

Укажите причину инцидента:

Повреждение/ Разрушение	
Кем	Тип
Работники / Посторонние / Природа	*Пожар / вода / ветер / молния / холод / жара / взрыв / транспорт / умышленный ущерб / другое*

Взлом	
Кем	Тип
Работники / Посторонние / Неизвестно	*НСД / сканирование / некорректное обращение с паролями / кража данных / разглашение данных / удаление данных / разрушение данных / отказ в обслуживании / другое*
Злоумышленное программное обеспечение	
Источник	Тип
Внутренний / Внешний / Неизвестно	*Вирус / червь / троянский конь / Spyware / Adware / Другое*
Наименование вируса	Кем
	Работники / администраторы / консультанты / дистрибутив ПО / игры / электронная почта / Web-сайт / коммуникации / другое / неизвестно
Кража	
Кем	Тип
Работники / Посторонние / Неизвестно	*Офисная кража / взлом / переезд офиса / при перевозке / внешняя кража / почта / другое*
Злоупотребление ресурсами / привилегиями / доверием	
Кем	Тип
Работники / Посторонние / Неизвестно	*Использование в личных интересах / использование в интересах третьего лица / установка ПО / изменение настроек ОС / мошенничество / вынос / отправка по электронной почте конфиденциальной информации / другое*
Ошибка персонала	
Кто ошибся	*Операторы / администраторы / программисты приложений / системные программисты / работники, управляющие коммуникациями / пользователи / посторонние / неизвестно / другое*
Повреждение/ авария/ выход из строя	
Чего	*Коммуникационное оборудование / информационная система / СУБД / сервис (служба) / линии связи / электроэнергия / кондиционеры / отопление / другое*
Другие причины	
Описание:	

Детализированная информация об инциденте

Привести описание инцидента

Как и почему произошел инцидент?

Привести причины возникновения инцидента, ход развития инцидента

Какие действия были приняты, когда инцидент произошел?

Привести действия по устранению инцидента

Какие действия планируются для снижения вероятности повторения инцидента и/или снижения ущерба инцидента при его повторении?

Привести запланированные корректирующие действия, сроки исполнения и ответственных

Любая другая важная информация:

Результаты анализа эффективности корректирующих действий:

Привести способ и результаты анализа эффективности выполненных действий

Офицер ИБ _____ _____ /_____/

(Дата) *(Подпись)*

Приложение 2
к Политике мониторинга
событий и управления
инцидентами ИБ

УВЕДОМЛЕНИЕ ОБ ИНЦИДЕНТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. **Инцидент информационной безопасности** – одно или серия событий ИБ, несущих угрозы ИБ Института.

2. **Основные типы** инцидентов информационной безопасности:

Инциденты информационной безопасности	Уведомляемые работники
Сбои в работе информационных систем и/или недоступность сервиса	– системный администратор; – офицер ИБ.
Выход из строя информационной системы	– системный администратор; – офицер ИБ.
Вредоносное ПО	– системный администратор; – офицер ИБ.
Нарушения политик и процедур ИБ	– офицер ИБ.
Несанкционированный доступ, утрата или кража конфиденциальной информации (в том числе персональных данных)	– офицер ИБ.
Недостатки в реализации систем ИБ	– офицер ИБ.

О возможных инцидентах Вам следует уведомить указанных выше работников по электронной почте или телефону.

3. Контактная информация

Офицер ИБ	
ФИО	
e-mail	
Рабочий телефон	
Мобильный телефон	
Ответственный специалист управления информатизации	
ФИО	
e-mail	
Рабочий телефон	
Мобильный телефон	

Приложение 3
к Политике мониторинга
событий и управления
инцидентами ИБ

ПЛАН РЕАГИРОВАНИЯ НА ИНЦИДЕНТ ИБ

РАЗРАБОТАН:

_____ _____
(дата) *(подпись)*

СОГЛАСОВАН:

_____ _____
(дата) *(подпись)*

_____ _____
(дата) *(подпись)*

УТВЕРЖДЕНО:
Проректор по информационным технологиям _____ _____
(дата) *(подпись)*

ОБЩАЯ ИНФОРМАЦИЯ

Наименование инцидента		
Ответственные за реагирование	*Должность*	*ФИО*
	Должность	*ФИО*
	Должность	*ФИО*
	Должность	*ФИО*
	Должность	*ФИО*

УСЛОВИЯ ЗАПУСКА ПЛАНА

№	Условие запуска плана	Источник информации	Критичность
1			
2			
3			
4			

ПОДГОТОВИТЕЛЬНЫЕ МЕРОПРИЯТИЯ

Условие запуска Плана	Источник информации	Подготовительное мероприятие	Пояснение	Ответственный

ДЕЙСТВИЯ ПРИ ВЫЯВЛЕНИИ ИНЦИДЕНТА

№	Действие	Ответственный	Временной норматив
1			
2			
3			

КОНТАКТНЫЕ ДАННЫЕ ОТВЕТСТВЕННЫХ ЛИЦ

ФИО	Роль	Контактные данные