Приложение № 18
к приказу № 78/2-ОД от 16.08.2021г

Регламент
реагирования на инциденты в информационной системе
МБДОУ «Ерёминский детский сад»

1. Общие положения

1.1. Настоящий Регламент реагирования на инциденты в информационной системе МБДОУ «Ерёминский детский сад» (далее – Регламент)устанавливает порядок действий при возникновении угроз информационной безопасности, обусловленных возможностью несанкционированного доступа к информационным ресурсам сторонних лиц (третьих лиц), внедрения и распространения вредоносного программного обеспечения, проведения массированных атак типа «отказ в обслуживании», а также возможными техническими сбоями в работе.

1.2. В Регламенте используются следующие понятия:

– инцидент информационной безопасности - любое непредвиденное или нежелательное событие, которое может нарушить деятельность информационных систем или информационную безопасность;

– информационное взаимодействие - процесс взаимодействия двух и более участников, целью которого является обработка информации в общих информационных системах и сетях;

– участники информационного взаимодействия - пользователи информационных систем (далее - пользователи), системные администраторы, администраторы безопасности.

1.3. Положения Регламента обязательны к соблюдению всеми сотрудниками, участвующими в выявлении, разбирательстве и предотвращении инцидентов информационной безопасности.

Задачи:

– определение порядка работы пользователей, системных администраторов и администраторов безопасности;

– обеспечение целостности, конфиденциальности и доступности информации;

– соблюдение требований правовых актов в области защиты информации.

2. Источники и виды инцидентов информационной безопасности

2.1. Источниками информации об инцидентах информационной безопасности являются:

– результаты работы средств мониторинга информационной безопасности, аудита (внутреннего или внешнего);

– журналы и оповещения операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем;

– обращения субъекта персональных данных с указанием инцидента информационной безопасности;

– иные источники информации.

2.2. Основными видами инцидентов информационной безопасности являются:

– несанкционированный доступ к информационным ресурсам;

– превышение полномочий - несанкционированный доступ к каким-либо ресурсам и помещениям сотрудников;

– компрометация учетных записей или паролей;

– вирусная атака или вирусное заражение;

– сетевые атаки (отказ в обслуживании (DoS-атаки), атаки типа Man-in-the-Middle, сниффер пакетов, переадресация портов, IP-спуфинг, атаки на уровне приложений и другое).

3. Анализ исходной информации

3.1. При получении информации о несанкционированном воздействии на информационную систему и сеть системный администратор ИС совместно с администратором безопасности ИС обязаны убедиться, что инцидент информационной безопасности не является результатом их собственной ошибки или санкционированных действий.

3.2. При выявлении инцидента информационной безопасности администраторам ИС необходимо:

– принять меры по пресечению несанкционированного воздействия в случае, если на момент выявления оно не завершено;

– принять меры по устранению причин возникновения инцидента информационной безопасности;

– сохранить образ или содержание информационной системы, в том числе журналы событий (информационного ресурса) на момент обнаружения события (несанкционированного воздействия);

– провести мероприятия по восстановлению работоспособности информационной системы (информационного ресурса);

– провести служебную проверку с целью выявления причин, которые могли привести к произошедшему несанкционированному воздействию.

3.3. Администратору безопасности ИС,необходимо в течение трех дней с момента обнаружения несанкционированного воздействия представить лицу, ответственному за защиту информации в ИС, результаты служебной проверки (наименование информационной системы (информационного ресурса), на которую произведено несанкционированное воздействие, время несанкционированного воздействия и (или) время обнаружения несанкционированного воздействия, местонесанкционированного воздействия (площадка, на которой размещается информационный ресурс, хостинг, краткое изложение (описание) произошедшего несанкционированного воздействия и информацию о последствиях несанкционированного воздействия, а также о принятых мерах по устранению причин несанкционированного воздействия).

3.4. По результатам рассмотрения полученной информации лицо, ответственное за защиту информации, в течение одного рабочего дня со дня ее получения принимает решение о необходимости внесения изменений в организационно-распорядительные документы.

3.5. Пользователь обязан:

– предоставлять свое автоматизированное рабочее место администратору безопасности для контроля;

– выполнять требования и рекомендации администратора безопасности и системного администратора;

– незамедлительно информировать администратора безопасности и системного администратора обо всех выявленных нарушениях, связанных с информационной безопасностью и обнаружением нештатного режима работы информационных систем и сетей.

3.6. Обязанности системного администратора:

– обеспечение бесперебойной работы системного программного обеспечения, серверного оборудования и автоматизированных рабочих мест пользователей;

– обеспечение резервного копирования данных (восстановление данных при необходимости);

3

– незамедлительное информирование администратора безопасности обо всех выявленных нарушениях, связанных с информационной безопасностью;

– осуществление мероприятий по предотвращению несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

– предотвращение незаконного вмешательства в информационные ресурсы и системы в иных формах;

– выполнение требований и рекомендаций администратора безопасности;

– ведение журнала учета инцидентов информационной безопасности (приложение № 1);

– принятие в течение одного рабочего дня мер по восстановлению работоспособности информационных ресурсов и информационных систем, согласуемых с администратором безопасности и вышестоящим руководителем (при необходимости);

– проведение совместно с администратором безопасности анализа зарегистрированных инцидентов информационной безопасности с целью разработки мероприятий (плана мероприятий) по их предотвращению.

3.7. Обязанности администратора безопасности:

– инструктаж пользователей по вопросам информационной безопасности;

– обеспечение функционирования установленных систем защиты информации;

– обновление антивирусных баз;

– проведение не реже 1 раза в год внутреннего аудита информационнойбезопасности;

– осуществление совместно с системным администратором при получении информации об инцидентах информационной безопасности мероприятий по предотвращению несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации, предотвращение других форм незаконного вмешательства в информационные ресурсы и системы;

– проведение совместно с системным администратором анализа зарегистрированных инцидентов информационной безопасности с целью разработки плана мероприятий по их предотвращению;

– осуществление контроля за: резервным копированием информации, сроками действия сертификатов соответствия средств защиты информации: ведением журнала учета инцидентов информационной безопасности;

– информирование непосредственного руководителя обо всех инцидентах, повлекших выход из строя или временную приостановку работоспособности автоматизированных рабочих мест и информационных систем (информационных ресурсов, серверного оборудования), а также о фактах несанкционированного воздействия, заражения вредоносными программами.

4. Ответственность участников информационного взаимодействия

4.1. Системный администратор, администратор безопасности и пользователи несут персональную ответственность за неисполнение или исполнение не в полном объеме своих обязанностей, указанных в разделе 3 Регламента.

Разработчик инструкции

заведующий МБДОУ «Ерёминский детский сад» Лукошенко Л.В.

Лист ознакомления с регламентом реагирования на инциденты в информационной системе МБДОУ «Ерёминский детский сад»

№ п/п	Ф.И.О. работника	Дата ознакомления	Личная подпись

Приложение № 1 к Регламенту
реагирования на инцидентыв
информационной системе МБДОУ
«Ерёминский детский сад»

Журнал учета инцидентов информационной безопасности

№ п/п	**Краткое описание инцидента**	**Фамилия, имя, отчество, должность сотрудника, обнаружившего инцидент, дата и время обнаружения**	**Дата и время пресечения несанкционированного воздействия**	**Дата, время направления сообщения об инциденте**	**Подпись системного администратора, администратора безопасности**	**Предпринятые действия для предупреждения возникновения инцидента**
1	2	3	4	5	6	7
		_____				