УТВЕРЖДЕНО
Приказ ректора университета
«29» апреля 2026 № 187-од

Регламент реагирования на инциденты информационной безопасности

1. Назначение документа

Регламент устанавливает порядок выявления, регистрации, классификации, обработки и расследования инцидентов информационной безопасности (далее – ИБ) в информационной системе университета.

Документ обязателен для всех сотрудников, администраторов и пользователей информационной системы (далее – ИС).

2. Термины и определения

Инцидент ИБ – событие или совокупность событий, приводящих или способных привести к нарушению конфиденциальности, целостности или доступности информации.

Специалист по защите информации – сотрудник, назначенный приказом ректора.

Администратор ИС – лицо, обеспечивающее техническое сопровождение ИС.

3. Цели реагирования

3.1. Минимизация ущерба от инцидента;

3.2. Предотвращение распространения угроз;

3.3. Восстановление работоспособности ИС;

3.4. Документирование действий;

3.5. Выполнение требований ОАЦ уведомлению и учёту.

4. Классификация инцидентов

Инциденты делятся на категории:

4.1. Критические

4.1.1 Внедрение вредоносного программного обеспечения на серверах;

4.1.2. Утечка персональных данных;

4.1.3. Компрометация учётных записей администраторов;

4.1.4. Атаки, приводящие к остановке ключевых сервисов.

4.2. Значимые

4.2.1. Заражение рабочих станций;

4.2.2. Массовые фишинговые рассылки;

4.2.3. Попытки подбора паролей;

4.2.4. Обнаружение уязвимостей.

4.3. Низкие

4.3.1. Единичные подозрительные события;

4.3.2. Ошибки пользователей;

4.3.3. Ложные срабатывания систем защиты.

5. Источники информации об инцидентах

5.1. Антивирусное программное обеспечение;

5.2. Система журналирования;

5.3. IDS/IPS;

5.4. Межсетевой экран;

5.5. Обращения пользователей;

5.6. Мониторинг сетевой активности;

5.7. Внешние уведомления (провайдер, CERT, ОАЦ).

6. Порядок реагирования на инциденты

6.1. Выявление

Инцидент может быть выявлен:

6.1.1. Автоматически (антивирусное программное обеспечение, IDS, SIEM);

6.1.2. Администратором;

6.1.3. Пользователем.

Обнаруживший обязан немедленно сообщить специалисту по защите информации.

6.2. Регистрация

Специалист по защите информации регистрирует инцидент в журнале:

6.2.1. Дата и время;

6.2.2. Источник;

6.2.3. Описание события;

6.2.4. Категория;

6.2.5. Принятые меры.

Журнал хранится не менее 1 года.

6.3. Первичный анализ

Специалист по защите информации определяет:

6.3.1. Тип инцидента;

6.3.2. Масштаб;

6.3.3. Затронутые ресурсы;
6.3.4. Необходимость изоляции.
6.4. Локализация
В зависимости от типа инцидента выполняются действия:
6.4.1. Отключение заражённого устройства от сети;
6.4.2. Блокировка учётной записи;
6.4.3. Остановка сервиса;
6.4.4. Фильтрация трафика;
6.4.5. Запрет внешних подключений.
6.5. Устранение последствий
6.5.1. Удаление вредоносного программного обеспечения;
6.5.2. Восстановление данных из резервных копий;
6.5.3. Обновление программного обеспечения и сигнатур;
6.5.4. Изменение паролей;
6.5.5. Исправление уязвимостей.
6.6. Восстановление работоспособности
После устранения последствий:
6.6.1. Проводится контрольное сканирование;
6.6.2. Проверяется целостность данных;
6.6.3. Устройство/сервис возвращается в эксплуатацию.
6.7. Расследование
Проводится анализ:
6.7.1. Причины инцидента;
6.7.2. Действия нарушителя;
6.7.3. Использованные уязвимости;
6.7.4. Эффективность мер защиты.
Результаты оформляются в отчёте.
6.8. Уведомление ОАЦ
Уведомление направляется в случаях:
6.8.1. Критических инцидентов;
6.8.2. Утечки персональных данных;
6.8.3. Атак, затрагивающих инфраструктуру университета.

7. Ответственность участников процесса

7.1. Пользователи обязаны:
7.1.1. Сообщать о подозрительных событиях;
7.1.2. Не предпринимать самостоятельных действий;
7.1.3. Соблюдать правила информационной безопасности.
7.2. Администраторы обязаны:
7.2.1. Выполнять локализацию и устранение последствий;
7.2.2. Вести журналы;

7.2.3. Обеспечивать мониторинг.
7.3. Специалист по защите информации обязан:
7.3.1. Координировать реагирование;
7.3.2. Проводить расследование;
7.3.3. Взаимодействовать с ОАЦ;
7.3.4. Готовить отчёты.

8. Документирование

По каждому инциденту оформляется:
8.1. Карточка инцидента;
8.2. Журнал регистрации;
8.3. Отчёт о расследовании;
8.4. Рекомендации по предотвращению повторения.

9. Профилактика инцидентов

9.1. Регулярное обновление программного обеспечения;
9.2. Обучение пользователей;
9.3. Тестирование резервного копирования;
9.4. Аудит конфигураций;
9.5. Анализ журналов;
9.6. Контроль внешних носителей.