УТВЕРЖДАЮ
Генеральный директор ООО «АЛЬТЕК»
М.Ю. Кожуховский

«08» декабря 2025 г.

СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ООО «АЛЬТЕК»

План реагирования на инциденты информационной безопасности

Санкт-Петербург, 2025

Оглавление

1. Введение 3
2. Обозначения и сокращения 3
3. Область действия 3
4. Роли и ответственность 3
5. Классификация инцидентов 3
6. Этапы реагирования 4
   6.1. Обнаружение и уведомление 4
   6.2. Регистрация и оценка 4
   6.3. Локализация 4
   6.4. Устранение 5
   6.5. Восстановление 5
   6.6. Анализ и предотвращение 5
7. Эскалация и информирование 5
8. Документирование 5
9. Контроль 6
10. Пересмотр плана 6

1. Введение

Настоящий План определяет порядок действий при выявлении инцидентов информационной безопасности (ИБ) с целью минимизации ущерба, восстановления работоспособности и предотвращения повторных инцидентов в ООО «Альтек».

План не является общедоступным документом, и не может предоставляться без ограничений всем заинтересованным сторонам. Решение о доступе к Плану третьих лиц принимает Руководитель по ИБ.

2. Обозначения и сокращения

ИБ	Информационная безопасность
ИА	Информационный актив
ИС	Информационная система
ПО	Программное обеспечение
СУИБ	Система управления информационной безопасностью

3. Область действия

План распространяется на:

- все информационные активы Компании;
- сотрудников организации и подрядчиков;
- технические и организационные инциденты ИБ.

4. Роли и ответственность

Роль	**Ответственность**
Сотрудник или подрядчик	Обнаружение и немедленное уведомление
Администратор ИБ	Регистрация, классификация, координация реагирования Техническая локализация и восстановление
Владелец ИА	Принятие решений по данным и доступам
Руководитель по ИБ	Утверждение мер, эскалация, отчетность

5. Классификация инцидентов

Инциденты классифицируются по типу:

- вредоносное ПО;
- несанкционированный доступ;
- утечка или компрометация данных;
- отказ или нарушение доступности ИС;
- фишинг и социальная инженерия;
- нарушение требований Политики ИБ.

Критичность инцидента определяется с учётом:

- уровня критичности затронутого информационного актива;
- потенциального ущерба для бизнес-процессов.

6. Этапы реагирования

6.1. Обнаружение и уведомление

Инцидент может быть выявлен:

- сотрудником;
- Администратором ИБ;
- средствами мониторинга и журналирования.

Все сотрудники и подрядчики обязаны незамедлительно уведомить об инциденте Администратора ИБ. Самостоятельные действия по устранению инцидента запрещены.

6.2. Регистрация и оценка

Администратор ИБ:

- регистрирует инцидент в журнале инцидентов ИБ;
- фиксирует затронутые ИА и ИС;
- определяет предварительный уровень критичности;
- уведомляет Руководителя по ИБ при значимых инцидентах.

6.3. Локализация

В зависимости от инцидента:

- изоляция рабочей станции или сервера;
- блокировка учетных записей;
- ограничение сетевого доступа;
- остановка уязвимых сервисов.

Возврат ИС в эксплуатацию осуществляется только после согласования

с Администратором ИБ и Руководителем по ИБ.

6.4. Устранение

- удаление вредоносного ПО;
- закрытие уязвимостей;
- смена скомпрометированных учетных данных;
- восстановление корректных конфигураций.

6.5. Восстановление

- восстановление данных и сервисов;
- проверка целостности и безопасности;
- возврат систем в эксплуатацию.

6.6. Анализ и предотвращение

По завершении реагирования:

- проводится анализ причин инцидента;
- оценивается ущерб;
- выполняется переоценка рисков в соответствии с Методикой оценки рисков ИБ;
- при необходимости актуализируется реестр рисков и планы их обработки.

7. Эскалация и информирование

При критичных инцидентах уведомляются:

- Руководитель по ИБ;
- руководство Компании.

В случаях, предусмотренных законодательством, могут быть также уведомлены внешние заинтересованные стороны.

8. Документирование

По каждому инциденту формируются:

- запись в журнале инцидентов;
- описание инцидента и принятых мер;
- результаты анализа и рекомендации;
- информация для последующего аудита ИБ.

9. Контроль

Инциденты ИБ и результаты реагирования:

- учитываются при проведении аудитов ИБ;
- используются для оценки эффективности мер защиты;
- являются основанием для корректирующих мероприятий.

Контроль выполнения мер осуществляется в соответствии с Методикой аудита ИБ.

10. Пересмотр плана

План пересматривается:

- не реже одного раза в год;
- после серьёзных инцидентов;
- при изменении ИТ-инфраструктуры или требований ИБ.