



Алгоритм действий
Работников объекта и иных лиц, находящихся на
объекте (территории), в случае несанкционированных
действий техническими способами (угрозе
несанкционированных действий)

Объект – строения (территория) Учреждения.

Оперативные службы — представители территориальных органов безопасности, Федеральной службы войск национальной гвардии Российской Федерации (подразделения вневедомственной охраны войск национальной гвардии Российской Федерации), Министерства внутренних дел Российской Федерации и Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий.

ИТ - инфраструктура — это совокупность всего программного обеспечения, оборудования, сетей и подключенных сервисов, образующих ИТ - среду организации. Каждый компонент ИТ - инфраструктуры предоставляет разные сервисы и повышает общую эффективность системы. Инфраструктура информационных технологий может состоять из следующих компонентов: серверы, персональные компьютеры, коммутаторы, маршрутизаторы, веб-серверы. Операционные системы, CMS, CRM-системы.

**Алгоритм действия руководителя
либо лица его замещающего.**

По предупреждению актов незаконного вмешательства:

- обеспечение безопасности сотрудников и антитеррористической защищенности критических элементов объекта (ГРЩ - главный распределительный щит, ВРУ- в водно-распределительное устройство, ИТП- индивидуальный тепловой пункт, и др.);
- организация и обеспечение охраны объекта, функционирования и контроля исправности инженерно-технических средств охраны, средств (систем) связи, оповещения, пожарной сигнализации качества их обслуживания;
- установление и поддержание на должном уровне пропускного и внутри объектового режимов;
- своевременное доведение до сотрудников и обеспечение контроля выполнения ими требований нормативных документов по противодействию терроризму;
- разработка соответствующих инструкций и памяток для персонала с учетом специфики объекта. Инструкции (памятки) о порядке действий персонала со схемами оповещения (телефоны дежурных (диспетчерских)служб по месту

расположения объекта) должны размещаться на информационных стендах в доступных для ознакомления;

- организация контроля безопасности служебных помещений с определением персональной ответственности;
- исключение возможностей проникновения на объект посторонних лиц через открытый подвал (люки, окна и т.д.);
- проведение комиссионных проверок помещений и прилегающих к объекту территорий для выявления уязвимых мест, причин и условий, способствующих осуществлению актов незаконного вмешательства, разработка и реализация мероприятий по их устранению;
- обеспечение режима защиты государственной и коммерческой тайны, в том числе работа с персоналом по вопросам сохранения в тайне особенностей функционирования на объекте системы охраны (защиты), ИТСО, средств оповещения, связи сигнализации;
- проводить тщательный подбор сотрудников, особенно обслуживающего персонала (дежурных, электриков, сантехников, ремонтников, уборщиков и др.);
- закрепление в договорах аренды (подряда) прав собственника на проведение проверок по соблюдению мер безопасности на объекте (его части);
- обеспечение постоянного взаимодействия с правоохранительными органами МЧС России.

По предупреждению хищения конфиденциальной информации:

- идентифицировать инцидент и убедиться, что он действительно имеет место быть;
- дать указание локализовать область ИТ - инфраструктуры, задействованной в инциденте и ограничить доступ к объектам, задействованным в инциденте;
- привлечь компетентных специалистов для консультации;
- создать группу по расследованию инцидента и составить план работ по сбору доказательств и восстановлению систем;
- протоколировать все действия, которые осуществляются в ходе реагирования на инцидент;
- в присутствии третьей независимой стороны произвести изъятие и опечатывание носителей информации с доказательной базой, а также снятие образцов и другой информации для последующего анализа и сохранения;
- оформить протоколом все операции с носителями информации;
- провести детальную опись объектов с информацией, извлекаемых данных, а также мест их сохранения, задокументировать процесс на фото/видеокамеру;
- после сохранения и оформления вещественных доказательств восстановить работоспособность информационных систем;
- при проведении расследования обеспечить корректное взаимодействие с заинтересованными правоохранительными органами и внешними организациями (компаниями, предоставляющие услуги в области расследования инцидентов информационной безопасности и обеспечения

по завершении расследования оформить соответствующий отчет и составить рекомендации по снижению рисков возникновения подобных инцидентов в будущем.

Алгоритм действия сотрудников (персонала), и иных лиц.

По предупреждению актов незаконного вмешательства:

- ежедневно тщательно осматривать свои рабочие места и, находясь на территории, обращать внимание на возможное обнаружение взрывного устройства или посторонних предметов, в том числе пакетов, свертков, коробок, а также на появление и поведение сторонних лиц;
- при обнаружении посторонних (подозрительных) предметов не подходить к ним, немедленно докладывать непосредственному руководителю или заместителю руководителя, принимать меры к ограничению доступа к этим предметам иных лиц;
- незамедлительно сообщать руководству о не исправности ИТСО, средств оповещения, связи сигнализации;
- не разглашать посторонним лицам информацию об особенностях охраны (защиты) объекта, функционирования ИТСО, средств оповещения и связи;
- немедленно сообщать непосредственному руководителю о лицах, проявляющих повышенный интерес к объекту и системе его охраны, а также о подозрительном поведении сторонних лиц на территории объекта.

По предупреждению хищения конфиденциальной информации:

- идентифицировать инцидент и убедиться, что он действительно имеет место быть;
- локализовать область ИТ-инфраструктуры, задействованной в инциденте;
- ограничить доступ к объектам, задействованным в инциденте;
- оформить служебную записку на имя руководителя о факте возникновения инцидента;
- обеспечить сохранность и должное оформление доказательств:
 - Собрать (сохранить, запротолировать, сфотографировать) всю доступную информацию об инциденте с работающей системы;
 - Собрать информацию о протекающем в реальном времени инциденте;
 - Отключить от сети питание;
 - Продолжить работу на автоматизированном рабочем месте только после восстановления работоспособности информационных систем и с разрешения руководства.