**Тема №2: Минимизация возможных последствий и ликвидация угрозы**

 **террористического акта. Система безопасности образовательного**

 **учреждения. Пути и способы проникновения на объект**

 **посторонних лиц.**

**1. Мероприятия по минимизации и (или) ликвидации последствий проявлений терроризма.**

Деятельность по минимизации и (или) ликвидации проявлений терроризма (далее - устранение последствий) планируется заблаговременно, исходя из прогнозов возможных последствий террористических актов. Эта деятельность должна быть ориентирована на решение следующих основных задач:

* недопущение (минимизация) человеческих потерь на основе приоритета защиты человеческой жизни перед материальными и финансовыми потерями (за исключением жизни террористов);
* своевременное проведение аварийно-спасательных работ и оказание медицинской и иной помощи лицам, участвующим в пресечении террористического акта, а также лицам, пострадавшим от террористического акта, их последующая социальная и психологическая реабилитация;
* минимизация неблагоприятных морально-психологических последствий воздействия террористических актов на общество или отдельные социальные группы;
* восстановление поврежденных и разрушенных объектов; возмещение причиненного вреда физическим и юридическим лицам, пострадавшим от актов терроризма (за исключением террористов).

Условиями успешного осуществления мероприятий по устранению последствий террористического акта являются учет специфики чрезвычайных ситуаций, связанных с совершением террористических актов, в зависимости от объектов посягательств и характера террористических воздействий, формирование типовых планов задействования сил и средств ОГСПТ и их заблаговременная подготовка, в том числе в ходе учений.

При возникновении ЧС возникает потребность в немедленном оповещении об опасности и информировании населения о действиях и мерах спасателей по оказанию помощи пострадавшим. Эти задачи решаются действиями сил и средств специализированных государственных организаций: пожарных, спасателей МЧС и ПСС, медиков, милиции с широким участием СМИ. Успешное решение задачи зависит от слаженности действий и комплексного подхода участников; учета особенностей возможных их видов; разнообразия последствий и необходимых мер противодействия и т. д. Наиболее уязвимыми объектами обеспечения информирования населения об опасности и выработки необходимых рекомендаций по защите от возникшей опасности являются сбор и обработка необходимой и достоверной информации о ЧС и ходе ее развития. Зачастую оповещение населения осуществляются с опозданием, в искаженном виде. В роли информаторов зачастую выступают люди или не обладающие достоверной информацией, или те, кто ею обладая, доводит ее до населения недостаточно своевременно, профессионально.

Ликвидация последствий чрезвычайной ситуации террористического характера должна представлять собой комплекс специальных мероприятий, осуществляемых с целью максимального ослабления поражения людей, снижения размеров материальных потерь и предотвращения возможного действия вторичного источника (взрыва заряда ВВ).

Основными задачами по ликвидации последствий чрезвычайной ситуации террористического характера являются:

* осуществление сбора, изучение, обобщение, оценка и предоставление информации о характере, масштабах, дальнейшем развитии и возможных последствиях чрезвычайной ситуации террористического характера;
* определение видов, объемов и трудоемкости работ по ликвидации последствий чрезвычайной ситуации террористического характера, а также потребного количества сил и средств для их выполнения;
* выдача экспертных заключений и предложений на использование тех или иных спасательных средств и инструментов, исходя из характера и масштабов чрезвычайной ситуации террористического характера;
* ведение разведки и контроля в районе ЧС террористического характера;
* проведение поисковых работ, в том числе с помощью служебных собак;
* проведение спасательных работ по извлечению пострадавших из-под завалов;
* оказание пострадавшим первой медицинской и врачебной с элементами специализированной помощи;
* проведение санитарной обработки личного состава спасательного центра и специальной обработки техники;
* участие в обезвреживании взрывных устройств.

Основными направлениями работ по противодействию терроризму и повышению уровня антитеррористической защищенности в субъектах Российской Федерации являются:

* разработка нормативных правовых и организационных документов по противодействию терроризму на объектах повышенной опасности, особой важности и жизнеобеспечения;
* проведение комиссионных обследований объектов повышенной опасности, особой важности и жизнеобеспечения;
* создание комиссий по антитеррористической деятельности;
* создание служб безопасности на объектах повышенной опасности, особой важности и жизнеобеспечения (систем физической защиты и охраны объектов);
* взаимодействие с органами МВД;
* информирование населения о правилах поведения при угрозе совершения терактов.

В соответствии с Федеральным законом РФ от 6 марта 2006 года №35 «О противодействии терроризму» в целях пресечения и раскрытия террористического акта, минимизации его последствий и защиты жизненно важных интересов личности, общества и государства может вводиться *правовой режим контртеррористической операции.*

Контртеррористическая операция проводится для пресечения террористического акта, если его пресечение иными силами или способами невозможно. Решения о проведении контртеррористической операции и о ее прекращении принимает руководитель федерального органа исполнительной власти в области обеспечения безопасности.

На территории (объектах), в пределах которой (на которых) введен правовой режим контртеррористической операции допускается применение следующих мер и временных ограничений:

1). проверка у физических лиц документов, удостоверяющих их личность, а в случае отсутствия таких документов - доставление указанных лиц в органы внутренних дел Российской Федерации (иные компетентные органы) для установления личности;

2). удаление физических лиц с отдельных участков местности и объектов, а также отбуксировка транспортных средств;

3). усиление охраны общественного порядка, объектов, подлежащих государственной охране, и объектов, обеспечивающих жизнедеятельность населения и функционирование транспорта, а также объектов, имеющих особую материальную, историческую, научную, художественную или культурную ценность;

4). ведение контроля телефонных переговоров и иной информации, передаваемой по каналам телекоммуникационных систем, а также осуществление поиска на каналах электрической связи и в почтовых отправлениях в целях выявления информации об обстоятельствах совершения террористического акта, о лицах, его подготовивших и совершивших, и в целях предупреждения совершения других террористических актов;

5). использование транспортных средств, принадлежащих организациям независимо от форм собственности (за исключением транспортных средств дипломатических представительств, консульских и иных учреждений иностранных государств и международных организаций), а в неотложных случаях и транспортных средств, принадлежащих физическим лицам, для доставления лиц, нуждающихся в срочной медицинской помощи, в лечебные учреждения, а также для преследования лиц, подозреваемых в совершении террористического акта, если промедление может создать реальную угрозу жизни или здоровью людей. Порядок возмещения расходов, связанных с таким использованием транспортных средств, определяется Правительством Российской Федерации;

6). приостановление деятельности опасных производств и организаций, в которых используются взрывчатые, радиоактивные, химически и биологически опасные вещества;

7). приостановление оказания услуг связи юридическим и физическим лицам или ограничение использования сетей связи и средств связи;

8). временное отселение физических лиц, проживающих в пределах территории, на которой введен правовой режим контртеррористической операции, в безопасные районы с обязательным предоставлением таким лицам стационарных или временных жилых помещений;

9). введение карантина, проведение санитарно-противоэпидемических, ветеринарных и других карантинных мероприятий;

10). ограничение движения транспортных средств и пешеходов на улицах, дорогах, отдельных участках местности и объектах;

11). беспрепятственное проникновение лиц, проводящих контртеррористическую операцию, в жилые и иные принадлежащие физическим лицам помещения и на принадлежащие им земельные участки, на территории и в помещения организаций независимо от форм собственности для осуществления мероприятий по борьбе с терроризмом;

12). проведение при проходе (проезде) на территорию, в пределах которой введен правовой режим контртеррористической операции, и при выходе (выезде) с указанной территории досмотра физических лиц и находящихся при них вещей, а также досмотра транспортных средств и провозимых на них вещей, в том числе с применением технических средств;

13). ограничение или запрещение продажи оружия, боеприпасов, взрывчатых веществ, специальных средств и ядовитых веществ, установление особого режима оборота лекарственных средств и препаратов, содержащих наркотические средства, психотропные или сильнодействующие вещества, этилового спирта, алкогольной и спиртосодержащей продукции.

На отдельных участках территории (объектах), в пределах которой (на которых) введен правовой режим контртеррористической операции, могут устанавливаться (вводиться) как весь комплекс мер и временных ограничений, так и отдельные меры, и временные ограничения.

В целях снижения риска возникновения и смягчения последствий террористических актов необходимо организация работы в соответствии с разработанным планом действий по предупреждению и ликвидации чрезвычайных ситуаций, вызванных террористическими актами, корректировка которого проводится ежегодно. Этим планом определены возможные места возникновения чрезвычайных ситуаций, меры по их ликвидации и решены вопросы взаимодействия с Управлением МВД России по г. Нижневартовск, отделом УФСБ, Управлением ГОиЧС, структурами Росгвардии в городе.

**2. Система безопасности образовательного учреждения.**

Именно повышению требований к защите социальных объектов – организаций системы Министерства просвещения посвящен подготовленный экспертами Правительства Российской Федерации документ, нормы которого введены в действие в августе 2019 года. Этот документ – *Постановление Правительства РФ от 02.08.2019 № 1006 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)» Положениями данного постановления утверждаются*[*требования*](http://base.garant.ru/71786064/#block_1000)*к антитеррористической защищенности объектов (территорий) Минпросвещения и объектов (территорий), относящихся к сфере деятельности этого ведомства, а также формы паспорта безопасности указанных объектов (территорий)*.

Новое постановление обновило требования, предъявляемые к образовательным объектам. Ранее проводилась реализация только требований, которые регулировались постановлением под №1235 от 7 октября 2017 г. Под действием нового закона оказалась сфера просвещения.

Требования, предусмотренные Постановлением Правительства России № 1006, устанавливают обязательные для выполнения организационные, инженерно-технические, правовые и иные мероприятия по обеспечению антитеррористической защищенности объектов.

Документом определяются принципы и порядок проведения категорирования объектов, подлежащее проведению для установления дифференцированных требований к обеспечению антитеррористической защищенности объектов с учетом потенциальной опасности и степени угрозы совершения террористического акта на объектах, значимости этих объектов для инфраструктуры и жизнеобеспечения и возможных последствий совершения террористического акта.

Постановление гласит, что руководство образовательной организации создает комиссию, которая займется обследованием и категорированием объекта. Комиссия включает, как правило, в себя представителей МЧС, ФСБ и Росгвардии, то есть членов силовых структур.
 В завершение обследования комиссия подготавливает соответствующий акт, который содержит информацию об обследовании и присвоении категории. Сведения в документе носят служебный характер, а иногда и секретный. Данная информация защищается законодательством Российской Федерации. Акт представляет собой важную часть будущего паспорта безопасности объекта образования. Составление данного документа укладывается в тридцать суток со дня подписания новоиспеченного акта. Паспорт формируют в 2-х экземплярах. Его согласуют с силовыми структурами в течение сорока пяти дней. В случае успешности процесса паспорт становится действительным на пять лет. Если изменилась площадь (периметр) или другие элементы, то паспорт должен обновляться и реорганизоваться.
 Требования устанавливают четыре категории террористической угрозы организаций. Категории соответствуют общему числу террористических акций, которые были совершены на территории, прилегающей к зданию. После формирования категории руководитель обязан создать паспорт в течение тридцати календарных дней. Также прописываются мероприятия, которые обеспечивают безопасность заведения от террористов. Каждая категория обладает своим перечнем. Обеспечение защиты подчиняется требованиям, согласно которым все инженерные системы согласованы с силовыми структурами.

Ответственным лицом за обеспечение безопасности образовательного процесса и антитеррористическая защищенность обучающихся и работников образовательного учреждения является заместитель директора ОУ по обеспечению безопасности, на которого возлагаются следующие обязанности:

1. Взаимодействие с территориальными подразделениями органов внутренних дел, гражданской обороны, федеральной службы безопасности, органом управления образованием, военным комиссариатом, другими органами и организациями, находящимися на территории муниципального образования по вопросам безопасности и антитеррористической деятельности.

2. Организация и обеспечение охранной деятельности и контрольно-пропускного режима.

3. Внесение руководителю (директору) предложений по совершенствованию системы мер безопасности и антитеррористической защищенности организации.

4. Разработка документов и инструкций по действиям личного состава в чрезвычайных и экстремальных ситуациях.

5. Принятие необходимых мер по оснащению организации средствами антитеррористической защищенности.

6. Организация функционирования предприятия (организации) при возникновении чрезвычайных ситуаций.

7. Разработка планирующей и отчетной документации по вопросам безопасности и антитеррористической защищенности.

Для образовательных учреждений актуально также обеспечение антитеррористической безопасности при проведении спортивно-массовых и культурно-зрелищных массовых мероприятий.

Планирование антитеррористических мероприятий осуществляется на полугодие или на квартал и включает:

- совещания АРГ по вопросам противодействия терроризму и экстремизму;

- инструктажи и тренировки;

- практические мероприятия по выполнению решений вышестоящих АРГ органов управления, - решений руководителя организации;

- меры по осуществлению контроля и оказания помощи на местах;

- работа по подготовке методических материалов, разработке инструкций и памяток.

Руководитель образовательного учреждения утверждает систему работы по противодействию экстремизму и терроризму, которая включает в себя:

* периодичность проведения совещаний, инструктажей;
* периодичность контроля выполнения основных мероприятий;
* организацию взаимодействия с ОВД, ФСБ, ГОЧС, и мероприятия, проводимые вместе с ними;
* сроки проведения различных культурно-спортивных и других массовых мероприятий, мероприятия по обеспечению безопасности их проведения;
* доклады о выполненных мероприятиях в вышестоящие инстанции;
* сроки представления информации и докладов антитеррористической рабочей группе.
* Планы действий (инструкции) по обеспечению безопасности персонала от проявлений терроризма могут быть составлены на базе материалов данного раздела.

Важно понимать, что все антитеррористические меры одновременно помогают защитить образовательную организацию от иных социальных, криминальных, техногенных и даже некоторых природных опасностей и ЧС.

Рекомендации руководителю по противодействию терроризму в условиях сохраняющей угрозы совершения террористических актов приоритетными считаются следующие задачи:

- воспитание чувства патриотизма, высокой бдительности, коллективизма, интернационализма и дисциплинированности;

- формирование культуры поведения, обеспечивающей собственную безопасность и безопасность окружающих.

Важно! Не исключается возможность вовлечения персонала организации в различные экстремистские, преступные организации и религиозные секты. Особенно этому подвержены учащиеся образовательных учреждений. Однако, нередки случаи участия в так называемых экстремистских организациях людей зрелого возраста.

Наиболее актуальными среди указанных направлений являются следующие:

* расширение и углубление знаний по вопросам предупреждения преступности и террористических актов;
* улучшение взаимодействия по предупреждению актов терроризма с управлениями ФСБ, ГОЧС, МВД, оказание практической помощи со стороны этих ведомств;
* активизация работы с персоналом и органами местного самоуправления по недопущению вовлечения (участия) в экстремистские и террористические организации;
* улучшение правового воспитания персонала, направленного на обеспечение их социальной, имущественной и личной безопасности;
* решительная борьба с проявлениями актов хулиганства, вымогательства, унижения, а также с употреблением наркотиков и алкоголя, с курением на территории организации.

Меры по усилению бдительности сотрудников в целях реализации мер по усилению бдительности, обеспечению безопасности жизни и здоровья сотрудников руководитель должен:

- изучить руководящие документы и методические материалы по предупреждению диверсионно-террористических актов;

- взять под личный контроль организацию антитеррористической защиты ОО, развернуть разъяснительную работу среди персонала ОО, обучающихся и их родителей, направленную на усиление бдительности, организованности, готовности к действиям в ЧС.

Особое внимание необходимо уделить реализации следующих мероприятий:

- совместно с представителями органов власти, средств массовой информации, Советами и Попечительскими советами, родителями провести комплекс предупредительно-профилактических мероприятий по повышению бдительности, обеспечению безопасности обучающихся и преподавателей;

- поддерживать взаимодействие с местными органами ФСБ, МВД, прокуратуры, военными комиссариатами и военным командованием;

- исключить возможность нахождения бесхозяйных транспортных средств в непосредственной близости и на территории;

усилить охрану ОО, организовать дежурство преподавательского и обслуживающего персонала;

- не допускать к ведению ремонтных работ рабочих, не имеющих соответствующих документов и согласований с органами управления образованием;

- обеспечить надежный контроль за вносимыми (ввозимыми) на территорию грузами (предметами) и своевременный вывоз твердых бытовых отходов;

- ежедневно проводить проверку подвалов, чердаков, подсобных помещений, держать их закрытыми на замок и опечатанными, проверять состояние решеток и ограждений;

входные двери держать в закрытом состоянии;

- обеспечить освещенность территории ОО в темное время суток;

- проверять наличие и исправность средств пожаротушения, тренировать внештатные пожарные расчеты;

- систематически корректировать схему оповещения сотрудников ОО;

- иметь в ОО план действий по предупреждению и ликвидации ЧС (в дошкольном ОО — инструкцию);

- обеспечить предупредительный контроль классов, аудиторий и помещений, где будут проводиться занятия, совещания, собрания, культурно-массовые мероприятия;

- довести до всех работников телефоны местных отделов ФСБ, МВД, прокуратуры, военного комиссариата, противопожарной службы, скорой помощи и аварийных бригад;

- о случаях обнаружения предпосылок к возможным террористическим актам, чрезвычайным происшествиям немедленно докладывать в органы правопорядка и управления образованием.

В целях уменьшения вероятности возникновения террористических актов рекомендуются следующие меры предупредительного характера:

- ужесточение элементов пропускного режима при входе и въезде на территорию объекта;

установка систем сигнализации, аудио– и видеозаписи;

- ежедневный обход территории и осмотр мест сосредоточения ценных или опасных веществ на предмет своевременного выявления ВУ или подозрительных лиц и предметов;

- периодическая комиссионная проверка складских помещений;

- более тщательный подбор и проверка кадров;

- организация и проведение совместно с сотрудниками правоохранительных органов инструктажей и практических занятий по действиям в ЧС;

- при заключении договоров на сдачу складских помещений в аренду в обязательном порядке - включать пункты, дающие право организации при необходимости осуществлять проверку сдаваемых помещений по своему усмотрению.

Полезно изучить помещения, узлы, агрегаты, установленные (построенные) в здании или вблизи его и по всему периметру. Выяснить, кем они обслуживаются (заняты), кто несет ответственность за их эксплуатацию и содержание. Следует узнать телефоны съемщиков и владельцев помещений и оборудования, телефоны вышестоящих организаций.

Рекомендуется:

- изучить места возможного заложения ВУ, складирования взрывоопасных веществ или создания взрывоопасных воздушных или сыпучих смесей;

знать в лицо работников коммунальных служб, обслуживающих объект;

- не оставлять без внимания появление посторонних лиц, не имеющих отношения к организации, их стремление обследовать объект, получить сведения о территории, режиме работы и сотрудниках;

- обращать особое внимание на стоянку незнакомых, безнадзорных автомобилей, загруженных или закрытых контейнеров и других подозрительных предметов;

- своевременно устанавливать и ремонтировать системы оповещения и взаимной информации, кнопки тревожной сигнализации.

По возможности лучше не использовать радиопереговорные устройства, чтобы исключить случайное срабатывание радиоуправляемого ВУ. Чтобы исключить срабатывание ВУ с магнитным типом взрывателя, не стоит приближаться к подозрительному объекту с металлическими предметами.

На открытой территории кроме специфических мест (для каждого конкретного объекта) в обязательном порядке осматриваются мусорные урны, канализационные люки, сливные решетки, цокольные и подвальные ниши, мусоросборники, закрытые киоски, сараи, посторонние машины, распределительные телефонные и электрощиты, водосливные трубы. Необходимо обращать внимание также на деревья, столбы, стены зданий, карнизы, крыши малоэтажных строений и т. п.

Необходимо иметь план осматриваемых помещений, знать расположение комнат, лестниц, ниш, силовых и телефонных коммуникаций, вентиляции, канализации. Это позволяет заранее предположить места возможных закладок. Необходимо также иметь комплект ключей от помещений, шкафов, ящиков столов и т. д.

Перед досмотром желательно обесточить внешнее электропитание. Если это по какой-либо причине затруднительно, то при осмотре стараться не включать досматриваемое оборудование.

При подозрении на наличие ВУ, открыть окна и двери в осматриваемых помещениях для рассредоточения возможной взрывной волны. Необходимо избегать резких непродуманных движений, особенно связанных с передвижением в пространстве и открыванием дверей, полок, нажатием выключателей и т. д.

**3. Модель нарушителя, возможные пути и способы его проникновения на охраняемый объект**

Как показывает опыт работы, нормальное функционирование системы защиты возможно при комплексном использовании всех видов защиты и четко спланированных действиях сил службы охраны по сигналам, получаемым от технических средств охранной сигнализации.

Охрана учреждения, как правило, является достаточно дорогостоящим мероприятием, поэтому при выборе уровня защиты целесообразно оценить возможные потери от "беспрепятственного" действия нарушителя и сравнить их с затратами на организацию охраны. Этот показатель является индивидуальным для каждого объекта и может быть оценен, как правило, весьма приближенно. Практика создания и эксплуатации комплексов технических средств охранной сигнализации показала, что в большинстве случаев для построения эффективной охраны требуется наличие комбинированных ТСОС, учитывающих возможность дублирования функций обнаружения на основе использования различных физических принципов действия средств обнаружения.

В основе эффективного противодействия угрозе проникновения нарушителя в охраняемые помещения лежит проведение априорных оценок:

- приоритетов в системе защиты;

- путей возможного проникновения нарушителей;

- информации, которой может располагать нарушитель об организации системы защиты предприятия;

- технических возможностей нарушителя и т.д., т.е. оценок совокупности количественных и качественных характеристик вероятного нарушителя.

Такая совокупность полученных оценок называется "моделью" нарушителя. Эта модель, наряду с категорией объекта, служит основой для выбора методов организации охраны объекта, определяет сложность и скрытность применяемых технических средств охранной сигнализации и телевизионного наблюдения, варианты инженерно-технической защиты, кадровый состав службы охраны и т.д.

По уровню подготовки и технической оснащенности "нарушителя" условно можно разделить на следующие типы:

- случайные;

- неподготовленные;

- подготовленные;

- обладающие специальной подготовкой и оснащенные специальными средствами обхода;

- сотрудники предприятия.

Наиболее распространенной "моделью" нарушителя является "неподготовленный нарушитель", т.е. человек, пытающийся проникнуть на охраняемый объект, надеясь на удачу, свою осторожность, опыт или случайно ставший обладателем конфиденциальной информации об особенностях охраны. "Неподготовленный нарушитель" не располагает специальными инструментами для проникновения в закрытые помещения и тем более техническими средствами для обхода охранной сигнализации. Для защиты от "неподготовленного нарушителя" часто оказывается достаточным оборудование объекта простейшими средствами охранной сигнализации и организация службы невооруженной охраны.

Более сложная "модель" нарушителя предполагает осуществление им целенаправленных действий, например, проникновение в охраняемые помещения с целью захвата материальных ценностей или получения информации. Для крупного учреждения наиболее вероятной "моделью" является хорошо подготовленный нарушитель, возможно действующий в сговоре с сотрудником или охранником. При этом возможны такие варианты проникновения, как:

- негласное проникновение одиночного постороннего нарушителя с целью кражи ценностей, для установки специальной аппаратуры или для съема информации;

- негласное проникновение нарушителя-сотрудника предприятия с целью доступа к закрытой информации;

- проникновение группы нарушителей в охраняемые помещения в нерабочее время путем разрушения инженерной защиты объекта и обхода средств охранной сигнализации;

- проникновение одного или группы вооруженных нарушителей под видом посетителей с целью силового захвата ценностей;

- вооруженное нападение на объект с целью захвата заложников, ценностей, получения важной информации или организации собственного управления.

Очевидно, "модель" нарушителя может предполагать и сразу несколько вариантов исполнения целей проникновения на 00.

Среди путей негласного проникновения нарушителя прежде всего могут быть естественные проемы в помещениях: двери, окна, канализационные коммуникации, кроме того непрочные, легко поддающиеся разрушению стены, полы, потолки. Поэтому при организации охранной сигнализации в охраняемом помещении в первую очередь должны быть установлены средства обнаружения для защиты окон и дверей. Обнаружение проникновения через стены, полы и потолки выполняют, как правило, СО, предназначенные для защиты объема помещения. Для усиления защиты окон и дверей широко используются металлические решетки и защитные жалюзи. Установка достаточно надежных решеток на окна может иногда позволить отказаться от установки на них средств охранной сигнализации. Однако часто наблюдалось, что неправильная конструкция решеток открывает дополнительные возможности для проникновения в здание. Например, защищая окна первого этажа, решетки могут облегчить доступ к окнам второго этажа.

Возможность проникновения на объект вооруженных нарушителей требует не только усиления вооруженной охраны, но и установки на входах обнаружителей оружия, оборудование особо ответственных рабочих мест сотрудников кнопками и педалями тревожного оповещения, а в ряде случаев и установки скрытых телекамер для наблюдения за работой сотрудников. Входы в хранилища ценностей должны оборудоваться специальными сейфовыми дверями с дистанционно управляемыми замками и переговорными устройствами.

Уровни технической оснащенности нарушителя и его знаний о физических принципах работы СО, установленных на объекте, определяют возможность и время, необходимое ему на преодоление средств инженерной защиты и обход сигнализационной техники. Наиболее эффективны СО, физический принцип действия и способ обхода которых нарушитель не знает. В этом случае вероятность его обнаружения приближается к единице.

В конечном счете, поскольку задачей системы охраны является оказание противодействий нарушителю в достижении его целей, при построении системы охраны в ее структуру закладывается принцип создания последовательных рубежей на пути движения нарушителя. Угроза проникновения обнаруживается на каждом рубеже и ее распространению создается соответствующая преграда. Такие рубежи располагаются последовательно от прилегающей к зданию территории до охраняемого помещения, сейфа. Эффективность всей системы защиты от несанкционированного проникновения будет оцениваться по минимальному значению времени, которое нарушитель затратит на преодоление всех зон безопасности. За это время, должна сработать система охранной сигнализации. Сотрудники охраны установят причину тревоги и примут необходимые меры.

Если "модель" нарушителя рассматривает негласное проникновение в охраняемое помещение нарушителя-сотрудника, в состав средств охранной сигнализации необходимо включить устройства документирования работы средств обнаружения, чтобы фиксировать несанкционированные отключения каналов сигнализации. Обычно указывается время постановки и снятия с охраны помещения. Аппаратура документирования должна устанавливаться в специальном помещении, куда имеют доступ только начальник охраны или ответственный сотрудник службы безопасности.

Итак, сложность системы охраны, ее насыщенность средствами инженерной и технической защиты определяются "моделью" нарушителя, категорией и особенностями объекта охраны. Количество необходимых зон безопасности определяется, исходя из состава материальных и информационных ценностей, а также специфических особенностей самого объекта. Если объект расположен в здании с прилегающей к нему территорией, то ограждение и периметральная охранная сигнализация образуют первую зону безопасности объекта. Последней зоной безопасности, например, сейфовой комнаты, будет специальный сейф с кодовым запирающим устройством и сигнализационным средством, передающим информацию о попытках его вскрытия.

Очевидно, что для разработки "модели" нарушителя применительно к некоторой 00 необходимо обобщение большого опыта как отечественной, так и зарубежной практики построения систем охраны объектов, аналогичных рассматриваемому. С течением времени "модель" нарушителя, а, следовательно, и вся концепция охраны могут меняться. Отсюда следует вывод о необходимости периодического дополнения концепции охраны объекта, обновления системы инженерной защиты, системы охранной сигнализации, телевизионного наблюдения, системы контроля доступа и всех иных систем, рассматриваемых системной концепцией обеспечения безопасности.

Способы получения "нарушителем" информации об объекте и технических способах защиты объекта, вероятные пути проникновения

Целями "нарушителя" или "нарушителей", проникающих на объект, как отмечалось выше, могут быть: кража материальных и/или информационных ценностей, установка закладных устройств, разрушение объекта, захват заложников, а возможно и захват управления функционированием объекта. Злоумышленник будет искать наиболее оптимальные пути проникновения в нужное ему помещение для осуществления поставленной противозаконной цели, будет стараться оставить как можно меньше следов своих действий, разрушений. С этой целью он будет изучать обстановку на объекте, алгоритм охраны, неохраняемые переходы, помещения, способы и условия хранения ценностей.

Применение систем охранной сигнализации с высокими тактико-техническими характеристиками на всех возможных путях движения "нарушителя" совместно с инженерной и физической защитой позволит достаточно надежно защитить объект на требуемом уровне.

Таким образом, неоспорима важность принятия мер, максимально затрудняющих получение "нарушителем" сведений об основных характеристиках технических средств охраны, их принципе действия, режимах работы.

В то же время некамуфлируемость средств охранной сигнализации в местах скопления посетителей, распространение слухов об их сложности, уникальности и невозможности их "обойти" будет способствовать отпугиванию некоторых потенциальных "нарушителей".

Наиболее вероятными путями физического проникновения "нарушителя" в здание являются:

- через двери и окна первого этажа;

- по коммуникационным и техническим проемам подвала или цокольного этажа;

- с крыши через окна или другие проемы верхних этажей;

- путем разрушения ограждений;

- имеются и иные способы, связанные с применением нарушителем специальных технических средств.

Необходимо максимально предусмотреть физические преграды перед нарушителем на пути его движения к материальным и информационным ценностям.

Внутренние переходы, подходы к наиболее важным помещениям должны быть оснащены не только средствами охранной сигнализации и телевизионного наблюдения, но и иметь надежную инженерную защиту в виде тамбуров с дистанционно управляемыми дверями, решетками, а сами хранилища ценностей - укрепленными перегородками.

Готовясь к преступлению, "нарушитель", используя легальную возможность посетить учреждение, ходит по некоторым его помещениям, может тщательно изучить наименее охраняемые места, расположение постов охраны, действия охранников при проходе сотрудников в различные режимные зоны. В этом случае очень важно разделять потоки клиентов учреждения от работников. Проходы, помещения, где клиенты не обслуживаются, должны иметь кодовые замки или средства контроля доступа.

Некоторые подробности режима охраны преступник может получить, "разговорив" кого-либо из работников учреждения или охраны.

Наибольшую опасность представляют сотрудники охраны, вступившие в преступную связь с "нарушителем". От них можно получить информацию и о принципах работы аппаратуры охранной сигнализации, ее режимах, "слабых" местах, оптимальных путях проникновения в требуемые помещения, а в решающий момент они могут отключить отдельные каналы охранной сигнализации. В связи с этим станционная аппаратура охранной сигнализации должна иметь систему документирования, должны протоколироваться дата и время включения/выключения каналов сигнализации, режимы проверки неисправности аппаратуры с фиксацией даты и времени происшедшего сбоя, отключения на профилактику и т.д.

Информация о состоянии охраны на объекте, оптимальных путях движения к требуемому помещению и путях отхода нужна любому "нарушителю", как стремящемуся похитить какой-либо документ, установить подслушивающее устройство, так и "нарушителю", осуществляющему разбойное нападение или преследующего иные цели.

Исходя из анализа возможных "моделей" нарушителя, способов получения им информации, конкретной архитектуры здания, характеристик территории, прилегающих зданий, рельефа местности и т.д., вырабатываются требования к инженерной защите, системе охранной сигнализации и размещению постов. Последнее означает, что для каждого конкретного объекта, здания, помещения должен разрабатываться конкретный проект его оснащения ТСОС-ТСН, СКД с учетом требований "Системной концепции...", дабы не допустить пробелов в системе защиты, которые раньше или позже, но будут обнаружены грамотным злоумышленником.

*Классификация нарушителей на основе моделей их действий*

Разработка моделей нарушителей осуществляется на основе исследования возможных видов угроз объекту и способов их реализации.

Угрозы могут носить общий или локальный характер и исходить:

- от людей;

- от природных факторов;

- от нарушения систем жизнеобеспечения из-за техногенных факторов, а также угрозы могут носить случайный характер.

При рассмотрении вопросов классификации нарушителей нас интересуют способы реализации угроз, исходящих от людей.

Рассматривают три типа нарушителей - неподготовленный, подготовленный, квалифицированный и две группы способов реализации угроз - контактные, бесконтактные.

Способы проникновения на объект, в его здания и помещения могут быть самые различные, например:

- разбитие окна, витрины, остекленной двери или других остекленных проемов;

- взлом двери, перепиливание дужек замка и другие способы проникновения через дверь;

- пролом потолка, подлежащего блокировке;

- пролом капитального потолка, не подлежащего блокировке;

- пролом стены, подлежащей блокировке;

- пролом капитальной стены, не подлежащей блокировке;

- пролом капитального пола, не подлежащего блокировке;

- пролом пола, подлежащего блокировке;

- проникновение через разгрузочный люк;

- проникновение через вентиляционное отверстие, дымоход или другие строительные коммуникации;

- проникновение подбором ключей;

- оставление нарушителя на объекте до его закрытия;

- свободный доступ нарушителя на объект в связи с временным нарушением целостности здания из-за влияния природно-техногенных факторов или в период проведения ремонта;

- проникновение через ограждение, используя подкоп, перелаз, разрушение, прыжок с шестом и т.д.

Очевидно, что каждый тип нарушителей будет осуществлять проникновение на объект по-разному - менее грамотно или более грамотно, используя различные условия, способствующие проникновению, как-то:

- взрыв;

- пожар;

- разбойное нападение;

- наводнение;

- химическое заражение;

- общественные беспорядки;

- отключение электроэнергии на объекте, в районе, городе;

- постановка нарушителем помех ТСО на объекте;

- постановка нарушителем помех в канале связи объекта с охраной;

- предварительный вывод из строя ТСО на объекте;

- предварительный вывод из строя канала связи объекта с охраной;

- предварительный сговор нарушителя с персоналом объекта;

- предварительный сговор нарушителя с персоналом службы охраны объекта;

- создание и использование многих и многих других условий для проникновения на охраняемый объект, например: использование дрессированных животных и птиц, специальных технических средств обхода ТСО, специальных технических средств для предварительного изучения объекта и т.д.

Ряд моделей действий нарушителей достаточно широко представлены в художественной литературе, кинофильмах, в телепередачах с криминальными сюжетами, в научно-технических изданиях в открытой печати. Таким образом, потенциальному злоумышленнику вполне доступно повышение квалификации на материалах открытой печати, телепередач и кино. Этот неоспоримый факт, безусловно, должна в своей деятельности учитывать СБ и соответственно строить тактику охраны учреждения. Очевидно, информация о тактике охраны является строго конфиденциальной, секретной и совершенно секретной.

В зависимости от поставленных целей злоумышленник создает те или иные условия для проникновения на объект и в его помещения, пользуясь теми или иными контактными или бесконтактными способами проникновения.

 К контактным способам совершения враждебных действий относятся:

1. Контактное проникновение на объект охраны:

- несанкционированное проникновение на территорию 00;

- проход на основе маскировки;

- установка средств негласного слухового, визуального, электромагнитного и др. наблюдения.

2. Контактное нарушение целостности или характера функционирования объекта:

- нарушение линий жизнеобеспечения 00;

- физическая ликвидация потенциала 00;

- затруднение штатного режима функционирования объекта.

 К бесконтактным способам совершения враждебных действий относятся:

1. Бесконтактные проникновения на объект охраны:

- перехват физических полей;

- контроль радио- и телефонных переговоров;

- визуальное и слуховое наблюдение;

2. Вывод объекта из строя без проникновения на него, как-то:

- нарушение целостности объекта посредством использования направленного взрыва или дистанционного оружия;

- отключение линий жизнеобеспечения объекта.

Нарушителем считается лицо, нарушающее контрольно-пропускной режим, случайно или преднамеренно нарушающее режим безопасности объекта охраны.

Для описания моделей нарушителей в качестве критериев классификации рассматриваются:

 1. Цели и задачи вероятного нарушителя:

- проникновение на охраняемый объект без причинения объекту видимого ущерба;

- причинение ущерба объекту;

- освобождение спецконтингента;

- преднамеренное проникновение при отсутствии враждебных намерений;

- случайное проникновение.

 2. Степень принадлежности вероятного нарушителя к объекту:

- вероятный нарушитель - сотрудник охраны;

- вероятный нарушитель - сотрудник учреждения;

- вероятный нарушитель - посетитель;

- вероятный нарушитель - постороннее лицо.

 3. Степень осведомленности вероятного нарушителя об объекте:

- детальное знание объекта;

- осведомленность о назначении объекта, его внешних признаках и чертах;

- неосведомленный вероятный нарушитель.

 4. Степень осведомленности вероятного нарушителя о системе охраны объекта:

- полная информация о системе охраны объекта;

- информация о системе охраны вообще и о системе охраны конкретного объекта охраны;

- информация о системе охраны вообще, но не о системе охраны конкретного объекта;

- неосведомленный вероятный нарушитель.

 5. Степень профессиональной подготовленности вероятного нарушителя:

- специальная подготовка по преодолению систем охраны;

- вероятный нарушитель не имеет специальной подготовки по преодолению систем охраны.

 6. Степень физической подготовленности вероятного нарушителя:

- специальная физическая подготовка.

|  |  |  |
| --- | --- | --- |
|  |  |  |