ГЛАВА 1

ПЛАНИРОВАНИЕ БЕЗОПАСНОСТИ

Оценка возможной угрозы проводится на основании жизненного опыта, объективных и субъективных факторов. При этом следует учитывать территориальное расположение, криминогенную обстановку в районе, где Вы живете и работаете, род Ваших занятий, контакты.

Достаточно много случаев, когда надежные, неправильно установленные технические средства, неправильное их использование либо отсутствие, позволяют преступникам проникать в дома, офисы или квартиры.

Летом и осенью по Киеву прокатилась волна компьютерных ограблений. Воровали самые дорогостоящие и малогабаритные компоненты.

Так в ночь с 23 на 24 октября 1995 года ограбили редакцию журнала «Hot Line». В результате неправильных действий охраны, преступники смогли заблокировать сигнализацию. За час были выпотрошены компьютеры. Преступники погрузили награбленное в две сумки, найденные в редакции, и скрылись через разбитое окно.

Количество ограблений не убывает. В ноябре того же года пострадала редакция газеты «Рейтинг». На втором этаже здания, арендуемого редакцией, ночью разбили стекло и проникли в помещение. Утром сотрудники не обнаружили принтера, сканера, радиотелефонов, факсов. Обнаружили разукомплектованный компьютер. Дежурные на первом этаже здания и соседнего магазина честно несли службу. И это в Киеве на Крещатике!

Офисы во многих случаях располагаются на первых этажах зданий. При неправильно установленных решетках, слабой двери или замке, даже при наличии сигнализации, у вас за 1,5-2 минуты могут вынести оргтехнику. При этом теряется информация, которая может представлять интерес для преступников и Ваших конкурентов.

В случае отсутствия сигнализации или охраны преступники беспрепятственно открывают дверь или окно, особенно, в плохо просматриваемых и неосвещенных местах.

Когда не удается отключить сигнализацию, сорвав или отогнув решетку, они разбивают окно и проникают в помещение. Одной-двух минут оказывается достаточно, чтобы унести несколько компьютеров.

Преступники используют как подручные средства, так и специальные. Их изобретательности нет предела. Они находят возможность подключения электроинструментов. Во время ограбления блокируют соседние двери с тем, чтобы их не застали на месте преступления. Вместо лестницы они могут использовать часть ограждения, ящики или бочки. В качестве лома – кусок арматуры или водопроводной трубы и так далее.

Приведенные примеры доказывают, что наличие только технических средств охраны не гарантирует вашу имущественную безопасность.

Действиям преступников, совместно с техническими средствами, следует противопоставить ряд организационных мер.

Опыт показывает, что среднее значение затрат на охрану материальных ценностей обычно не превышают десяти процентов их стоимости.

Организационные меры не требуют больших материальных затрат, но их эффективность подтверждена жизнью и часто недооценивается потенциальными жертвами.

Отметим их одну отличительную особенность в сравнении с техническими средствами: организационные меры никогда не становятся провоцирующим фактором агрессии. Они применяются до столкновения с преступником. Последний не может воспользоваться их преимуществами, как в случае, например, самообороны с применением оружия.

Соблюдение основных принципов и простых правил позволит Вам предотвратить возможный материальный, моральный ущерб, финансовые потери и инциденты на работе и дома.

Потенциальные жертвы недооценивают важность организационных мер. Происходит это потому, что их выполнение нельзя осуществить техническими средствами.

К организационным мерам относятся:
– оценка возможной угрозы;
– выбор мер по охране квартиры, дома, автомобиля, служебных помещений;
– выбор режима работы;
– подбор кадров и т. д.

Одной из первых организационных мер, которую осуществляет каждый в разной степени – оценка возможной угрозы. Делать это лучше не ожидая ограбления. С такой оценкой сталкивается каждый человек при получении квартиры, выборе помещения под офис, склад и т. д. Степень угрозы определяется наличием ценностей.

Ценности, требующие охраны, могут быть материальными и нематериальными. К нематериальным ценностям относится, например, информация.

При защите помещений задачу следует решать комплексно, чтобы не переделывать несколько раз дизайн помещения и коммуникации. Все системы должны устанавливаться с учетом следующих факторов:
– обеспечения надежности;
– обеспечения стоимости;
– удобства использования;
– возможного их влияния друг на друга;
– возможность модернизации.

Заметим, что даже ограбление не всегда вдохновляет потерпевших и их соседей установить сигнализацию. В большинстве случаев ограничиваются рядом минимальных дополнительных мер. Если ограничиться только укреплением дверей и решеток, это не гарантирует Вас от повторного «посещения».

При удавшемся ограблении преступники время от времени наблюдают за потерпевшим и спустя, например, полгода – опять могут проверить прочность Ваших дверей и решеток. На это их «вдохновляет» удачная попытка.

Не следует забывать о противопожарной безопасности. Статистика показывает, что потери от пожаров значительно превосходят убытки от хищений.

Наиболее гибкими, не требующими прокладки коммуникаций, являются беспроводные системы. Это могут быть охранные, противопожарные устройства и системы телевизионного наблюдения. С их описанием мы познакомимся в третьей и четвертой главах.

Даже ограбление не всегда вдохновляет потерпевших и их соседей установить сигнализацию

Многие предпочитают не думать о возможных криминальных событиях, так как в постоянной тревоге жить невозможно. Но беспечность и разобщенность людей ведут к тяжелым, чаще всего невосполнимым потерям.

Основное во взаимных отношениях правоохранительных органов с населением – это взаимная информация. Огромное количество преступлений предотвращается или быстро раскрывается, когда в обществе установилась привычка немедленно сообщать о фактах готовящихся правонарушений или преступлений, подозрительных лицах.

В цивилизованных странах контакты с полицией не считаются зазорными, а у нас в милицию обращаются не желая ей хоть чем-нибудь помочь, считая что Ваша беда – это их работа. Улучшению ее работы в немалой степени может способствовать помощь граждан.

1.1. ОЦЕНКА ПОТЕНЦИАЛЬНОЙ УГРОЗЫ И ВЫБОР АДЕКВАТНЫХ СРЕДСТВ ЗАЩИТЫ

Организационные меры связывают в единое целое все составляющие безопасности. Правильность выбора и проведения организационных мер определяет степень Вашей безопасности.

Оценка степени безопасности

Для оценки степени безопасности, предлагаем Вам ответить на ряд вопросов:

- Достаточно ли надежно охраняется ваше оборудование, ценности, информация?
- Работает ли сигнализация?
- Какие противопожарные мероприятия Вы проводите?
- Как будет действовать охрана, если сработает сигнализация?
- Где хранятся документы и резервные копии информации?
- Насколько просматриваются помещения снаружи и из каких мест?
- Имеете ли вы резервные копии информации?
- Как скоро вы сможете восстановить работоспособность своей фирмы, если случится ограбление?

Это не банальные вопросы. Дешевле учиться на чужих ошибках.

Помните! Квалификация преступников растет с каждым ограблением.

Затраты на дополнительные защитные устройства или модернизацию старых несоизмеримо малы, в сравнении с ущербом от одного единственного взлома или пожара.

При оборудовании помещений охранными системами обращайтесь к специалистам, а не к умельцам. Последние очень дешево выполнят любые работы, но не могут дать никаких гарантий.

Если охранные устройства установлены, Вы должны всегда их правильно использовать. Потратьте время на тренировку. Этим вы оградите себя от потрясений, которые не доставляют радости.

Безопасность информации

С развитием рыночных отношений, появлением частных предприятий, предприниматели столкнулись с новой проблемой, связанной с обеспечением не только имущественной безопасности, но и с безопасностью информации.

Информация – очень емкое понятие. В нашем случае под информацией понимается коммерческая информация и ее несанкционированное получение.

Не существует четкой границы между информацией доступной всем и коммерческой информацией. Само по себе любое сообщение не имеет ценности без факта передачи его кому-либо. Поэтому защита информации заключается в передаче сообщений только тому лицу, которому она адресована.

В последние годы приобретает все большую актуальность защита от несанкционированного доступа компьютерной информации.

Появление локальных и глобальных компьютерных сетей, электронной почты, широкого обмена информацией и программными продуктами привело к возможности несанкционированного доступа к информационным системам банков, страховых компаний, и как следствие – к похищению безналичных средств и коммерческих секретов.

В Украине стремительно развивается сфера услуг, которая специализируется на сборе и обработке коммерческой информации. В этих условиях защита информации не может осуществляться на любительском уровне.

При планировании защиты информации необходимо решить следующие вопросы.

1. Определить информацию, подлежащую защите.
2. Оценить возможный ущерб от утечки информации.
3. Оценить необходимую степень защищенности каналов и носителей информации.

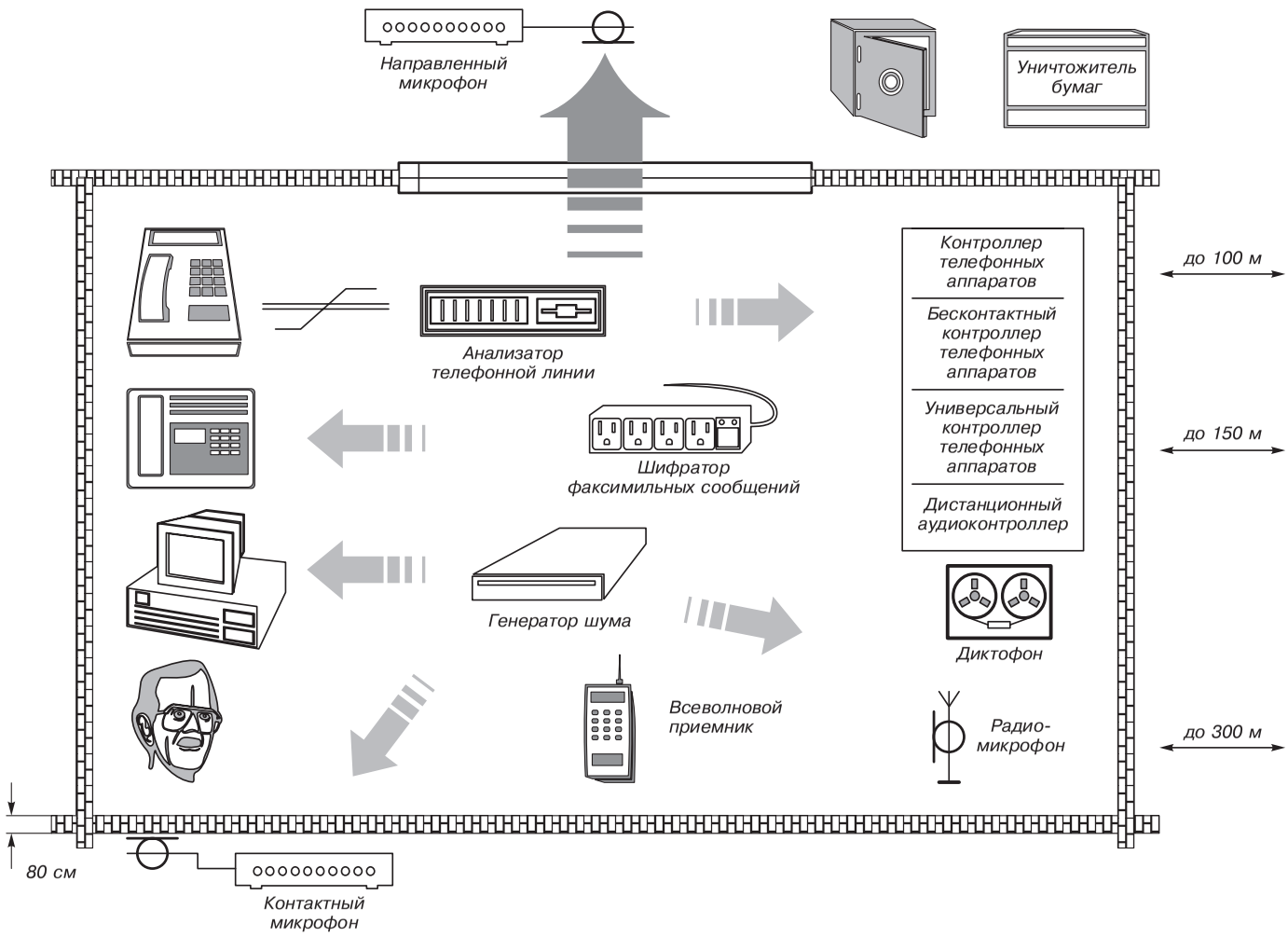

Рис. 1.1. ***Каналы утечки информации***

Безопасность интерьера

Представить каким образом Ваша безопасность связана с интерьером вашего предприятия помогут ответы на следующие вопросы:

– Остаются ли ваши посетители одни?
– В каком виде выбрасываются черновики записей, фотокопии телефаксов и прочие бумаги?
– Защищены ли данные в памяти компьютера паролем?
– Контролируется ли доступ к компьютеру извне?
– Как хранятся копии важной информации?
– Закрываются ли на ключ все важные документы в конце дня?
– Какие участки помещения просматриваются снаружи?
– Какие стены вашего кабинета доступны снаружи?
– Используются ли вами радиотелефон?

Безопасность помещения непосредственно связана с безопасностью информации.

Источники информации, доступные техническим средствам, графически представлены на рис. 1.1 слева.

Справа на рисунке расположены устройства, используемые для прослушивания помещений.

В центре рисунка находятся устройства индицирующие, блокирующие и предотвращающие прослушивание и утечку информации.

Часть попыток несанкционированного съема информации можно обнаружить техническими средствами, используя аппаратуру поиска, обнаружения и локализации активных технических средств.

Часть можно предупредить с помощью технических средств обеспечения скрытности передачи информации. Используя генераторы шумовых помех в радио и акустическом диапазонах, возможно блокирование различных подслушивающих устройств.

Правильность выбора технических устройств защиты информации во многом определяет их эффективность.

Решить вопросы безопасности Вы можете создав службу безопасности, прибегнув к услугам охранных фирм или, наконец, воспользовавшись здравым смыслом и собственным опытом.

С техническими средствами защиты, используемыми при передаче информации, вы познакомитесь в пятой главе. Там же представлены технические характеристики средств обнаружения и защиты от несанкционированного съема информации.

Определившись в выборе средств защиты, следует проконсультироваться со специалистами, которым вы безусловно доверяете.

Осуществив разграничение полномочий и доступ к информации, можно избежать ее утечки. Каждый должен получать только ту информацию, которая позволяет ему работать с наибольшей эффективностью

Соблюдение мер безопасности

Контролировать утечку информации достаточно легко. Самыми рискованными точками являются:

– места скопления информации (архивы, мусор и т. д.);
– потоки информации, иногда слишком большие, чем это необходимо (официальные документы, посетители, временные сотрудники);
– распределители информации (секретарь, вспомогательный персонал руководства)

Для существенного ограничения утечки информации следует выполнять ряд простых мер [2].

1. Установите режущий аппарат вблизи копировального и выработайте в себе и своих сотрудниках привычку уничтожать все ненужные документы.
2. Защитите посредством паролей данные в памяти компьютера.
3. Контролируйте доступ к компьютеру извне. Самая простая процедура состоит в запрещении пользования на протяжении определенного времени и задания сигнала тревоги, если три попытки набора кода ошибочны.
4. Периодически делайте копии охраняемой информации и помещайте их в надежное место.

5. Ограничьте выход информации до минимума.
6. Для того чтобы кого-либо ввести в заблуждение, информацию можно подвергнуть некоторой упаковке:

– под-информация – дается информация правдивая, но разрозненная или неполная, или слишком общая;
– сверхинформация – дается большое количество информации, но часть ее является бесполезной или ложной, но преподноситься так, чтобы это было невозможно обнаружить.

7. Ограничьте места приема посетителей и не оставляйте их одних.
8. Не злоупотребляйте набором временных сотрудников, которые часто имеют доступ к большому количеству информации. Остерегайтесь особенно тех «студентов», которым под сорок.
9. Дайте секретарю указание осаждать лиц, обнаруживающих интерес к необычной информации.
10. Закрывайте на ключ все важные документы в конце рабочего дня. Ничего, нигде не должно валяться.
11. Телефоны, телефаксы, телексы должны рассматриваться с точки зрения безопасности передачи информации. Следует применять код для сообщения особо важной информации (например, цены в ответе на коммерческое предложения).

Необходимо регулярно вновь и вновь повторять всем, от простого служащего до руководящего состава, элементарные меры безопасности. С этой точки зрения поведение руководства является основным.

Бдительность должна начинаться с головы и распространяться по всему организму до тех пор, пока не станет рефлексом.

Такой результат не достигается без усилий, но, в конце концов, выгода берет верх над небольшими неудобствами в самом начале.

Эти меры эффективны, но нельзя забывать, что хранить тайну, в конце концов, должны сами люди.

Никакая система кодирования ничего не стоит, если вдруг встретишь сочувствующее ухо соседа по бару, ощутив себя крайне одиноким после неурядицы дома или на работе

Иначе говоря, все служащие, а в особенности те, которые находятся вблизи источников информации, должны отдавать себе отчет в том, что они могут невольно провоцировать утечку информации. Это относиться и к наивным инженерам, которые обсуждают с другом повышение по службе; менеджеру, хвастливо говорящему слишком много в ходе выставки; секретарше, которая делиться со своим женихом, не говоря уже о коммерсанте, вверяющем свои секреты покупателю.

Большая часть утечки информации происходит из-за небрежности. Так что защита, прежде всего, дело обучения.

Однако бдительность не должна принимать характер паранойи. Разумеется, есть много случаев утечки информации. Если кто-либо задастся такой целью, он найдет средства пробить ту трубу, по которой циркулирует информация и получит то, что желает, как бы тщательно эта информация не была сокрыта.

1.2. СТРАХОВАНИЕ

Одной из форм защиты собственности является страхование. Страхование не уменьшает степень угрозы, а позволяет компенсировать, полностью или частично, потери в результате, например, хищения имущества. Поэтому страхование является дополнительной мерой по повышению Вашей имущественной безопасности.

Страхование – одна из категорий общественных отношений. Оно постепенно стало непременным спутником любого производства. Первоначальный смысл слова страхование связан со словом «страх».

Владельцы имущества, вступая между собой в производственные отношения, испытывали страх за его сохранность, за возможность уничтожения или утраты в связи со стихийными бедствиями, пожарами, грабежами и другими непредвиденными опасностями.

Рискованный характер производства – главная причина беспокойства каждого собственника за свое материальное благополучие. На этой почве закономерно возникла идея возмещения материальною ущерба путем солидарной его раскладки между заинтересованными владельцами.

Если бы каждый отдельно взятый собственник попытался возместить ущерб за свой счет, то он был бы вынужден создавать материальные или денежные резервы, равные по величине стоимости своего имущества.

Между, тем жизненный опыт, основанный на многолетних наблюдениях, позволил сделать вывод о случайном характере наступления чрезвычайных событий и неравномерности нанесения ущерба.

Было замечено, что число заинтересованных лиц часто бывает больше числа пострадавших от различных опасностей. При таких условиях солидарная раскладка ущерба между заинтересованными лицами заметно сглаживает последствия различных случайностей. При этом, чем большее количество лиц участвует в раскладке ущерба, тем меньшая доля средств приходится на одного участника. Так возникло страхование, сущность которого составляет замкнутая раскладка ущерба.

Раскладка ущерба в денежной форме создавала широкие возможности, прежде всего, для взаимного страхования, когда сумма ущерба возмещалась его участниками на солидарных началах либо после каждого страхового случая. Взаимное страхование стало закономерно перерастать в самостоятельную отрасль.

Если при взаимном страховании еще не формировался заранее рассчитанный страховой фонд, то в дальнейшем вероятная средняя величина возможного ущерба, приходящаяся на каждою участника страхования, стала применяться в качестве основы страховых взносов для заблаговременного формирования страхового фонда.

Авторы не ставили своей целью подробно освещать вопросы страхования. Эта страница – напоминание читателям о замечательной возможности компенсации любого ущерба

Термин «страхование», выражающий перераспределительные отношения по поводу возмещения ущерба, следует отличать от других смысловых значений этого слова. В частности, выражение «страхование» (страховка, подстраховка) иногда употребляется в значении поддержки в каком-либо деле, гарантии удачи в чем либо, обеспечения безопасности.

Перераспределительные отношения, присущие страхованию, связаны, с одной стороны, с формированием страхового фонда с помощью заранее фиксированных страховых платежей, а с другой – возмещением ущерба из этого фонда участникам страхования.

В международной страховой практике документ, который включает пункты, регулирующие основные условия страхования называется страховым полисом.

1.3. СЛУЖБЫ БЕЗОПАСНОСТИ

Информация предоставлена ***ЗАО «Производственная фирма «ALLETA»***

В условиях кардинальной перестройки экономики и существенных изменений общественных отношений в Украине возникли и быстро развиваются структуры негосударственных охранных служб, которые на основе организационно-правового регулирования призваны обеспечивать цивилизованное развитие рынка услуг по охране частного и государственного имущества как от посягательства уголовного элемента, так и от такого бедствия, как пожар.

Фирма, оборудованная сигнализацией, не вызывает желания у малолетних или несовершеннолетних преступников совершать акты разбоя или вандализма.

Безусловно, что при массовом возникновении организаций, претендующих на столь ответственную деятельность, как охрана жизни и собственности, существует вероятность внедрения в ряды профессионалов, прямо скажем, безответственных низкоквалифицированных работников.

Рост численности подобных фирм объясняется стремительным ростом потребностей внутреннего рынка в охранных системах, кстати сказать, совпадающим с «бумом» на мировом рынке производителей подобных систем. Возросшая потребность объясняется как объективной необходимостью, соответствующей СНИПам и украинским стандартам, так и факторами психологического направления.

Деятельность фирм по защите информации лицензируется Государственной службой Украины по вопросам технической защиты информации.

Система лицензирования деятельности охранных служб является определенным барьером на пути подобных элементов, но не может полностью гарантировать клиента от установки низкокачественной, морально устаревшей или дорогостоящей аппаратуры не отвечающей своим функциональным назначением задачам охраны конкретного объекта.

Эти сбои понятны, так как «слабая» в финансовом плане организация не может содержать специалистов по изучению рынка современных технических средств, проводить сертификацию нового оборудования, обеспечивать обслуживание нетрадиционных систем. Современные средства охраны, включающие программирование, инсталляцию и компьютерные сети, защиту от саботажа, модульное проектирование и наращивание функционирующих систем, требуют квалифицированного обслуживания.

Потенциальному заказчику необходимо не только убедиться в наличии лицензии, дающей формальное право на производство работ, но не постесняться ознакомиться и с конкретными исполнителями и производственной деятельностью фирмы.

АО «Аллета» полностью принимает на себя ответственность не только за безопасность клиента, но и за финансовую сторону выполнения заказа. Самое современное оборудование – за возможно низкую цену – таков девиз предлагаемых специалистами фирмы проектов.

Для этого отдел маркетинга фирмы постоянно пополняет банк данных по выпуску на мировой рынок охранно-пожарных систем сигнализации и стремится получить непосредственно от производителя первые образцы новых разработок.

Фирма поддерживает непосредственные контакты с такими лидерами мирового уровня, как японская фирма «Optex», швейцарские фирмы «Galica» и «Erapa», немецкие – «Total Walter» и «Esser», канадская – «Greenel», словенская «Zarja-Electronica».

Специалисты фирмы прошли обучение на словенской, швейцарской и немецкой фирмах и получают постоянную методическую поддержку из учебных центров этих фирм.

В заключение можно подчеркнуть, что АО «Аллета» высоко ценит свое членство в Украинской федерации негосударственных служб безопасности, поскольку это является лучшей рекомендацией профессионализма, добросовестности и ответственности.

Таблица 1.1.

Стоимость основного оборудования проводной системы сигнализации	
Однокомнатная квартира	$550…650
Двухкомнатная квартира	$650…800
Трехкомнатная квартира	$800…1200
Стоимость монтажа определяется количеством охраняемых зон	

Таблица 1.2.

Стоимость основного оборудования беспроводных систем сигнализации для офисов, коттеджей квартир и промышленных объектов	
Inter-guard 1000	$3500…4500
Inter-guard 2000	$4000…5000
Multi-guard 3000	$15000…25000
Стоимость ретрансляторов	$350
Стоимость охранных и пожарных датчиков	$350…450
Стоимость монтажа зависит от количества охраняемых зон и составляет 30...40% от стоимости основного оборудования	

Таблица 1.3.

Стоимость основного оборудования систем охраны периметра (OPTEX)	
Условная стоимость комплекта на 100м охраняемой площади	$3500…3700
оборудование OPTEX	–
кабельная продукция	–
строительные работы	–
Стоимость монтажа составляет 40-60% от стоимости оборудования	

Таблица 1.4.

Стоимость основного оборудования систем Protectowire	
Стоимость комплекта:	$3500…12000
концентратор	$800…2500
датчики	$35…100
кабель «Protectowire» (за 1 погонный метр в соответствии с условиями эксплуатации)	$7…15
Условная стоимость комплекта пожаротушения	
Газовые системы пожаротушения на 100м^3 объема	$4500…5000
цена определяется газонаполнением системы	
Водяные системы пожаротушения на 100м^2 площади	$3500…4000
цена определяется электрической системой управления	
Пенные системы пожаротушения на 100м^2 площади	$4500…5000
цена определяется высотой помещения и технологическим оборудованием	

Таблица 1.5.

Стоимость основного оборудования систем видеонаблюдения	
Стоимость комплекта:	$1000…1500
условный монитор	–
четыре камеры	–
соединители	–
Стоимость монтажа составляет 25-30% от стоимости оборудования	

Основные затраты на оборудование и виды услуг по фирме «АЛЛЕТА» представлены в таблицах 1.1...1.5.

В таблицах приведены средние цены в условных единицах и ориентировочные стоимости монтажа оборудования.

Специалистами фирмы для Вас будет разработан проект и подобрано соответствующее оборудование.

В третьей главе Вы можете ознакомиться с описанием охранных, противопожарных устройств и систем ограничения доступа, предлагаемых АО «Аллета».

Особое внимание рекомендуем обратить на противопожарные датчики точечного и линейного контроля помещений. Системы, оборудованные такими датчиками, обладают наивысшей надежностью, так как постоянно контролируют их состояние.

Стоимость систем ограничения доступа высока. По этим вопросам следует получить консультацию у специалистов фирмы.