Глава

1

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ СОЗДАНИЯ И ПРИМЕНЕНИЯ СИСТЕМЫ ЗАЩИТЫ ОБЪЕКТОВ

1.1. ЦЕЛИ, ЗАДАЧИ И ЭТАПЫ СОЗДАНИЯ И ПРИМЕНЕНИЯ СИСТЕМЫ ЗАЩИТЫ

Безопасность объектов организации (предприятия) обеспечивается комплексом организационных (оперативных, режимных) и технических (инженерно-технических, пожарно-профилактических) мероприятий и действий физических лиц (сотрудников охраны, администрации и т. д.), направленных на предотвращение ущерба интересам предприятия и его персоналу в результате хищения материально-технических и финансовых средств, уничтожения имущества и ценностей, разглашения, утраты, утечки и уничтожения информации, нарушения работы технических средств [1]—[6].

Главной целью любой системы безопасности является обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности от противоправных посягательств, а также недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение нормальной производственной деятельности всех подразделений объекта, как в условиях повседневной деятельности, так и в чрезвычайных ситуациях.

Достижение заданной цели возможно в ходе решения следующих *основных задач*:

- прогнозирование и своевременное выявление угроз безопасности, как самому объекту, так и информационным ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;
- категорирование объектов предприятия;
- разработка концепции безопасности и политики безопасности предприятия;
- создание условий (реализация концепции), обеспечивающих предупреждение и ликвидацию угроз безопасности объекту, его информационным ресурсам и нанесения различных видов ущерба;
- создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы, основываясь на правовых, организационных и технических мерах и средствах обеспечения безопасности;
- создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности на достижение стратегических целей.

Обеспечения безопасности конкретного объекта (предприятия) необходимо начинать с разработки концепции обеспечения безопасности (или концепции безопасности — КБ), в которой формулируется целостное, системное представление о системе защиты объекта.

Концепция обеспечения безопасности — это научно обоснованная система взглядов на создание целостной системы безопасности объекта, определяющая цели, задачи, принципы и способы защиты объектов, включающая анализ и оценки угроз, особенности объекта защиты и выражающая общий замысел организации и реализации мер различного характера для обеспечения защиты объекта от возможных угроз (создание системы безопасности) и оценку эффективности их применения.

Содержание и взаимосвязь отдельных разделов концепции обеспечения безопасности предприятия (объекта) показаны на рис. 1.1.

Рис. 1.1. Содержание и взаимосвязь отдельных разделов концепции обеспечения безопасности предприятия (объекта)

Разработка концепции безопасности преследует две основные цели.

1. Выработка общей точки зрения по обеспечению безопасности предприятия (объекта) между руководством, его сотрудниками и фирмами, привлекаемыми для организации безопасности, производства работ по техническому оснащению объекта и др.

2. Создание основы организации режимов, обеспечивающих безопасность, и принятие управляющих решений по финансированию соответствующих программ.

Этапы создания и модернизации системы безопасности определяются значимостью факта ее создания (степень угрозы), рисками и предполагаемыми потерями. Особенности эксплуатации системы физической защиты характеризуются особенностями применения и построения используемых систем контроля и управления доступом (СКУД) и технических систем и средств охраны, контроля и сигнализации.

В разработке концепции безопасности объекта можно выделить три основных этапа.

На ***первом этапе*** осуществляется подготовка исходных данных, заключающаяся в сборе следующих документов и материалов:

- подробные планы территории и поэтажные планы помещений объекта защиты с указанием их функционального назначения и строительных особенностей;
- схемы коммуникаций (энергоснабжение, телефонная связь, теплоснабжение, внутренние компьютерные сети и пр.) с указанием способа их прокладки;
- чертежи, рисунки или фотографии мест, представляющих опасность с точки зрения несанкционированного проникновения на объект (туннели тепловых и водопроводных коммуникаций, тонкие стены, граничащие с чужой территорией, переходы с крыши на крышу, подвальные помещения, холодильные установки, бойлерные, электрощитовые и др.);
- перечень особенностей эксплуатации зданий и сооружений объекта, влияющих на режим безопасности (права арендодателей помещений, необходимость посещения различными инспекциями и т. п.);
- схема режима освещенности территории в ночное время;
- схема организации движения транспорта по объекту и территории, прилегающей к нему;
- нормативный документ, определяющий режим работы сотрудников, и правила посещения объекта клиентами.

На ***втором этапе*** специальная экспертная группа, формирующая концепцию безопасности, и руководство предприятия принимают основополагающие решения по вопросам безопасности:

- формируется список возможных угроз, представляющих опасность интересам предприятия на данном этапе его работы и развития;
- решается вопрос о том, какими силами предполагается осуществлять охрану объекта (собственными силами, с помощью правоохранительных органов или охранных агентств);
- определяются допустимые пределы режимных ограничений, которые не нанесут ущерба основной деятельности предприятия;
- оцениваются допустимые пределы возможного финансирования программ, связанных с обеспечением безопасности;
- определяются приоритеты и ориентировочные сроки их реализации.

На ***третьем этапе*** разрабатываются документы, составляющие основу концепции:

- таблицы с описанием помещений, здания и участков территории с указанием режимности (рекомендуется градация степени режимности из шести категорий);
- схема (план) охраны объекта с указанием маршрутов движения сотрудников, расположения постов охраны, распределение функций между постами охраны и техническими средствами усиления безопасности;
- документация по созданию контрольно-пропускного режима с иерархией доступа различных категорий клиентов и сотрудников в помещения с разной степенью режимности;
- оценка необходимости и принципов защиты коммуникаций;
- определение необходимости усиления защищенности объекта техническими средствами (укрепление строительных конструкций, система охранной сигнализации, телеНаблюдения, устройство контроля и регистрации и т. д.) и составление структурной схемы технического оснащения;
- оценка необходимости и разработка системы предотвращения утечки информации с объекта;
- принципы локализации возможного ущерба от происшествий и чрезвычайных ситуаций;
- рекомендации по порядку взаимодействия с правоохранительными организациями в ситуациях возникновения угрозы безопасности и при расследовании происшествий;
- сметы расходов на выполнение необходимых проектных, монтажных и других работ с указанием ориентировочной стоимости необходимого оборудования и расходов на эксплуатацию или просто определение максимально допустимых пределов расхода средств на эти цели;
- перечень организаций, которые могут быть привлечены для осуществления мероприятий по организации защиты объекта.

В зависимости от характера работы предприятия и его структурной организации в концепцию могут включаться и другие разделы.

1.2. АНАЛИЗ УЯЗВИМОСТИ ОБЪЕКТОВ И РИСКОВ ПОТЕРИ РЕСУРСОВ

Все объекты, которые могут подвергнуться угрозам безопасности или противоправным посягательствам, имеют различную потенциальную уязвимость с точки зрения возможного

информационного, материального или морального ущерба. Под *уязвимостью объекта понимается степень его незащищенности от воздействия нарушителей*. Уязвимость зависит от эффективности системы защиты (СЗ) объекта, т. е. степени его защищенности от нарушителей. Анализ уязвимости объекта включает 4 этапа (рис. 1.2):

1) разработка модели действий нарушителей;

2) выявление и оценка основных видов угроз и возможного ущерба от их реализации;

3) оценка показателей уязвимости объекта и существующей системы безопасности, выделение особо важных зон и объектов, категорирование особо важных объектов;

4) оценка рисков потери ресурсов организации, на основании чего определяются пути нейтрализации угроз и формируются общие рекомендации по обеспечению безопасности объекта.

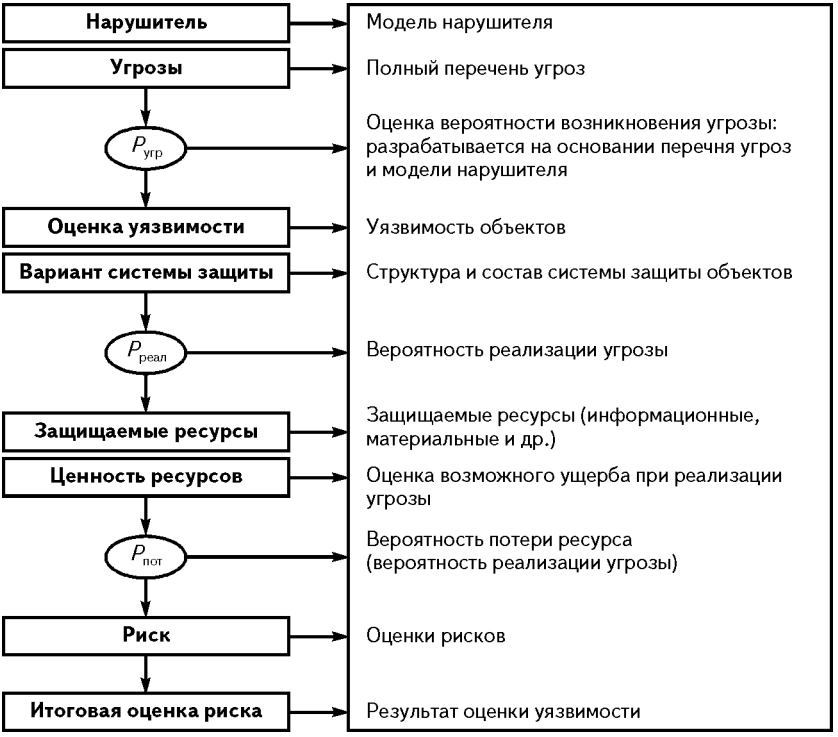

Рис. 1.2. Этапы оценки уязвимости объекта и рисков потери ресурсов

К *объектам, подлежащим защите* от потенциальных угроз и противоправных посягательств, относятся:

- персонал организации — носители информации (руководящие работники, производственный персонал, имеющий непосредственный доступ к информации, финансам, ценностям, хранилищам, осведомленный о сведениях, составляющих государственную и коммерческую тайну, работники внешнеэкономических служб и др.);
- информационные ресурсы с ограниченным доступом, составляющие государственную, служебную и коммерческую тайну, а также иная конфиденциальная информация на бумажной, магнитной, оптической основе, информационные массивы и базы данных, программное обеспечение, секретная и конфиденциальная документация;
- средства и системы информатизации (автоматизированные системы и вычислительные сети, средства вычислительной техники, линии телеграфной, телефонной, факсимильной, радио- и космической связи, технические средства передачи информации, средства размножения и отображения информации, вспомогательные системы);
- финансово-экономические ресурсы, обеспечивающие эффективное и устойчивое развитие предприятия;
- материальные ресурсы (здания, сооружения, хранилища, важное технологическое оборудование, готовая продукция, интеллектуальная собственность, транспорт и иные средства);
- технические средства и системы охраны и защиты информационных и материальных ресурсов.

Основными угрозами безопасности, которые могут привести к утрате ресурсов предприятия, являются:

- чрезвычайная ситуация;
- несанкционированный съем конфиденциальной информации;
- хищение или порча имущества;
- ухудшение эффективности функционирования и устойчивости развития.

Особое внимание уделяют защите от чрезвычайных ситуаций.

На этапе анализа совместно со службой безопасности заказчика при предварительном обследовании объекта формируется модель вероятных исполнителей угроз (нарушителей), т. е. их количественные и качественные характеристики (оснащенность, тактика действий и т. п.).

1.3. МОДЕЛИ НАРУШИТЕЛЕЙ

Под ***моделью нарушителя*** понимается описательная характеристика, отражающая его возможный моральный облик, уровни физической подготовленности, знаний, обученности и оснащенности, которые дают возможность оценить степень способности и заинтересованности в преодолении системы защиты предприятия, с одной стороны, а с другой, — определить допустимый уровень инженерно-технической подготовленности рубежей существующей (модернизируемой) системы безопасности.

Модель нарушителей включает:

- категории (типы, классы) нарушителей, которые могут воздействовать на объект;
- цели, которые могут преследовать нарушители каждой категории, возможный количественный состав, используемые инструменты, принадлежности, оснащение, оружие и другое снаряжение (техническая вооруженность);
- типовые сценарии возможных действий нарушителей, описывающие последовательность действий групп и отдельных нарушителей, способы их действий на каждом этапе.

В модели следует учитывать как *внешних* нарушителей, проникающих на территорию, в зоны, здания и помещения объекта и его информационные ресурсы (ИР) извне, так и *внутренних*, т. е. из числа штатного персонала объекта или посетителей, имеющих возможность легальным путем получить допуск на объект. Необходимо также учитывать возможность сговора и совместных действий внешних и внутренних нарушителей.

Случайный нарушитель не имеет преступных намерений, не знает оборудования, не применяет подручных средств для проникновения, не пользуется специальными приемами проникновения в охраняемую зону. Задача системы защиты, применяемой против этого типа нарушителя, — обнаружить наиболее простые, открытые формы проникновения.

Преступник-дилетант решается на преступление при появлении благоприятного момента. Он не знает оборудования, используемого для защиты, может применять подручные средства для проникновения, будет осторожен при проникновении. На такого нарушителя ориентированы основные технические средства защиты и сигнализации.

Подготовленный нарушитель способен выявить и определить по внешнему виду тип оборудования, знает принципы его работы, размеры и форму зон обнаружения. Он может найти и ис-

пользовать характерные для данного оборудования и ИС уязвимые места, применить подручные средства для проникновения и обхода предполагаемой зоны обнаружения, умышленно вызвать ложные срабатывания оборудования, при наличии доступа способен подручными средствами вывести его из строя.

Профессиональная преступная организация может иметь в своем распоряжении необходимые финансовые, человеческие и технические ресурсы для подготовки скрытого вторжения на охраняемый объект. Она имеет возможность провести детальное изучение объекта, разработать и реализовать проекты нейтрализации оборудования. Такой организации можно противопоставить только сложные инженерно-технические комплексы в сочетании с высокой закрытостью информации о способах их применения.

Для любого объекта можно выделить классы нарушителей, действия которых наиболее вероятны. Для каждого класса характерны свои способы действий, цели, задачи и соответственно методы противодействия им. К характеристикам нарушителей, позволяющим описать их основные классы относят:

- мотивы (цели);
- объемы финансового обеспечения;
- наличие и уровень профессиональной подготовки;
- техническое обеспечение;
- качество предварительной подготовки преступления;
- уровень внедрения нарушителей на объект.

Мотивы (*цели*) *действий* нарушителей:

- желание приобрести материальные ценности (в т. ч. деньги);
- конкурентная борьба;
- сведение личных счетов;
- политические и религиозные мотивы;
- любопытство;
- ошибка;
- неосознанные немотивированные действия (влияние алкоголя, наркотических веществ).

Схема *финансового обеспечения* деятельности нарушителей варьируется в самых широких пределах. В общем случае выделяют 3 уровня финансового обеспечения:

1) практически неограниченное;
2) ограниченное;
3) отсутствие финансирования.

Неограниченное финансирование присуще спецслужбам различных государств, международным террористическим органи-

зациям и т. п. Ограниченное финансирование характерно для борьбы небольших конкурирующих организаций. Финансовое обеспечение отсутствует у нарушителей-одиночек и случайных нарушителей.

Наличие и уровень профессиональной подготовки нарушителей зависит от финансового обеспечения, но не связан с ним напрямую. Понятно, что организации, обладающей достаточным финансовым обеспечением, проще найти профессионалов в любой области. Однако хороший уровень профессиональной подготовки может быть, и у небольшой группы. Много преступлений совершают одиночки, хорошо подготовленные профессионально, в том числе самоучки. Существуют криминальные группы, сумевшие получить финансирование, но не имеющие достаточной профессиональной подготовки.

Техническое обеспечение гораздо больше, чем профессиональная подготовка, связано с финансированием. Во многих случаях для преодоления систем безопасности требуется дорогостоящее оборудование и материалы, в том числе:

- оборудование и оснастка для разрушения и других способов преодоления технических укреплений;
- контрольно-измерительная аппаратура для обнаружения и идентификации технических средств;
- аппаратура для блокирования технических средств;
- вооружение (для террористов — взрывчатые вещества).

Наличие и качество предварительной подготовки преступления определяет эффективность действий нарушителя. Подготовка преступления включает целый ряд вопросов: планирование, разведка, внедрение на объект, проведение предварительной работы по блокированию технических средств и т. п. Выделяют 3 класса подготовки преступления: долговременная, оперативная подготовка и отсутствие подготовки.

Долговременная подготовка наиболее эффективна — она позволяет провести весь комплекс подготовительных операций вплоть до внедрения в структуру объекта. Время, закрученное на нее, может колебаться от нескольких недель до нескольких лет. *Оперативная подготовка* включает в первую очередь техническую оснащенность группы нарушителей. Она может длиться от нескольких часов до нескольких недель. Чаще всего за это время сложно обеспечить внедрение на объект, провести соответствующую разведку и техническую подготовку на объекте. *Отсутствие подготовки* характерно для случайных преступлений, совершаемых одиночками или небольшими группами.

Наличие и уровень внедрения нарушителей на объект не обязательно зависят от предварительной подготовки. Во многих случаях преступления совершают сами сотрудники объектов. Причем преступниками могут являться люди, занимающие любые должности — вплоть до высшего руководства. Выделяют 2 класса внедрения на объект:

1) *случайное внедрение* — нарушители изначально работают на объекте не с целью совершения преступлений;

2) *целенаправленное внешнее внедрение* — нарушители внедряются на объект с заранее поставленной целью — совершение преступления.

Учитывая вышесказанное, можно выделить несколько классов нарушителей, характеризуемых следующими особенностями действий (табл. 1.1):

- *класс А* — нарушители, действующие злонамеренно и обладающие практически неограниченным финансовым обеспечением;
- *класс Б* — нарушители, действующие злонамеренно и обладающие ограниченным, но достаточным финансовым обеспечением;
- *класс В* — нарушители, действующие злонамеренно, обладающие малым (или вообще никаким) финансовым обеспечением, но имеющие хороший профессиональный уровень подготовки;
- *класс Г* — нарушители, действующие злонамеренно, обладающие малым (или вообще никаким) финансовым обеспечением и имеющие низкий уровень профессиональной подготовки;
- *класс Д* — нарушители, действующие незлонамеренно.

В модели нарушителя также отражаются *способы действий* нарушителя применительно к используемым техническим средствам защиты периметра, территории и зданий. Так, если исключить экзотические случаи (например, дельтаплан), то существует 4 реальных вида вторжения:

- «пересечение» рубежа: бег, ходьба, медленный шаг, ползком, прыжком, перекатом;
- «перелаз» заграждения (с помощью и без помощи подручных средств);
- «пролаз» через заграждение путем деформирования или разрушения полотна заграждения;
- «подкоп» под заграждение, техническую систему охраны (ТСО).