Защита объектов. Теория и практика

Владимир Викторович Маликов, начальник цикла технических и специальных дисциплин в УО «Учебный центр Департамента охраны» МВД Республики Беларусь

Практическое обеспечение информационной и инженерно-технической защиты объектов не возможно без построения системы безопасности на определенной методологической основе. Конечно, положения действующих НПА (ТНПА) могут обозначить общее направление построения систем защиты на академически структурированной основе, однако в настоящее время существует значительный разрыв в теории и практике обеспечения безопасности. Зачастую практические аспекты опережают развитие теоретических подходов, что заставляет представителей служб безопасности решать возникающие проблемы только на основе имеющейся совокупной базы знаний. Иногда эти решения носят инновационный характер, а зачастую это просто решение вопросов на «горящей основе» со сроками реализации проблемы на день, неделю, месяц. Ликвидность принятых решений по безопасности значительно влияет на общий тренд обеспечения устойчивой финансово-экономической деятельности объекта.

1. Краткая характеристика типового объекта как объекта защиты.

Начальным аспектом, определяющим общую структуру построения системы безопасности, является проблема четкого понимания того, что необходимо защищать. Построение общей схемы функциональных связей финансово-экономической деятельности объекта позволяет выделить элементы сопряжения с вопросами обеспечения безопасности. Сначала то, что необходимо защищать, затем — как защищать. Перечень ресурсов объекта, подлежащих защите, определяет общий уровень сложности построения системы безопасности, а также потребности в применении необходимых методических подходов. Часто вопросы обеспечения безопасности локализуются ровно по степени понимания проблемы руководством компании и только потом службой безопасности. Обеспечение информационной безопасности без сопряжения с вопросами контроля физического доступа к объекту/ресурсам объекта зачастую приводит к дублированию соответствующих позиций в бюджетах, выделяемых на безопасность. Так, если на уровне государства (Республика Беларусь) имеется более 25 НПА (ТНПА), дублирующих вопросы обеспечения комплексной безопасности, то на уровне конкретного объекта данное дублирование приводит к значительным финансовым потерям. Сколько же стоит экономически оправданная безопасность? Создатель экономически оправданной системы защиты, ориентируясь на уровень мировых показателей, может обеспечить варьирование критериев показателей (затрат на их обеспечение) от 15 до 25 % от совокупной стоимости ресурсов объекта подлежащего защите.

Структура типового объекта как объекта защиты включает в себя следующие элементы:

а) земельные участки, предназначенные для размещения объекта:
— территория, на которой располагаются основные здания, помещения;
— территория, на которой располагаются вспомогательные элементы инфраструктуры объекта: разгрузочные площадки, проезды и тротуары, зеленые насаждения и др.;
б) терминалы доступа на территорию объекта:
— для прохода посетителей и персонала;
— для проезда на территорию автомобилей.
в) системы холодного и горячего водоснабжения, канализации и водостоков:
— с выходом за территорию периметра объекта;
— без выхода за территорию периметра объекта.
г) системы отопления, вентиляции и кондиционирования воздуха:
— с выходом за территорию периметра объекта;
— без выхода за территорию периметра объекта.
д) системы естественного и искусственного освещения зданий;
е) системы электроснабжения электротехнических устройств:
— автономные;
— централизованные, с дополнительным резервированием;
ж) каналы связи и коммуникации:
— вычислительных сетей;
— сетей связи и автоматизации.
з) здания, помещения объекта:
— помещения с общим доступом персонала и посетителей;
— режимные помещения с особыми условиями доступа персонала и посетителей, объекты обработки конфиденциальной информации (объекты информатизации);
и) пути транспортирования ценностей:
— по зданиям, помещениям объекта;
— по территории периметра объекта.

2. Среда защиты типового объекта.

2.1 Характеристика потенциального нарушителя.

Социально-психологический портрет нарушителя, мотивация и обеспечение — все указанные позиции уже изначально профессионально проработаны и используются в практической деятельности сотрудников ведомств силового блока. Не секрет, что именно эти сотрудники, уже выйдя на пенсию, формируют основу руководства служб безопасности.

Организация и ведение аналитической работы определенного уровня требует значительного финансирования. Однако руководитель компании зачастую не может принять решения по выделению значительных средств на сопровождение процесса обеспечения защиты, не представляя четкой структуры практического использования собранных оперативных

материалов. Четко и внятно изложить функциональные связи, затрагивающие вопросы безопасности, по силам считанным руководителям служб безопасности, как правило, бывшим сотрудникам МВД, КГБ, МЧС, в связи с тем, что зачастую каждый из них ранее был жестко привязан только к одному-двум элементам структуры безопасности и потенциально не способен понять конечную цель достижения определенного уровня комплексной защиты.

Основные мотивы нарушителя: приобретение материальных ценностей, конкурентная борьба, сведение личных счетов, политические мотивы, религиозные мотивы, любопытство, немотивированные действия под влиянием алкоголя и/или наркотических веществ.

Основные цели нарушителя: кража материальных ценностей, получение информации, уничтожение материальных ценностей, уничтожение информации, создание помех функционированию объекта.

Финансовое обеспечение нарушителя: практически не ограниченное, ограниченное или полностью отсутствует.

Наличие и уровень профессиональной подготовки нарушителей: высокий, средний и низкий.

Техническое обеспечение:

— 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;

— взрывчатые вещества и др.

Наличие и качество предвари**тельной подготовки преступления:** долговременная подготовка преступления или оперативная подготовка преступления.

Наличие и уровень внедрения нарушителей на объект: целенаправленное внешнее внедрение или его отсутствие.

К основным нарушителям могут относиться следующие группы организаций: организованные криминальные структуры, конкурирующие организации государственного масштаба (крупные концерны, холдинги; крупные банки и т. п.).

2.2 Предположения.

Построение системы безопасности невозможно без постановки перечня формализованных задач, что определяет конкретные бюджеты для их решения. Зачастую само построение финансово-экономической деятельности объекта имеет очень «размытую» структуру, что изначально предполагает множество потенциальных инцидентов безопасности.

Система безопасности не предназначена для решения всех адресных вопросов, связанных с персоналом объекта, имеющимися экономическими схемами функционирования компании, схемами логистики и др. Естественно, что при любом значимом инциденте безопасности сотрудники службы безопасности почти всегда будут выступать в роли виновного: «куда смотрели?», «для чего вы нужны?». Однако уже изначально руководитель службы безопасности должен сформировать свой перечень условий и предположений, при котором выполнение поставленных задач представляется возможным.

В перечень предположений включим наиболее существенные и наиболее полно характеризующие среду защиты типового объекта, а именно:

— предположения о предполагаемых условиях эксплуатации объекта;

— предположения о физической защите среды безопасности объекта;

— предположения относительно пользователей, администраторов безопасности и обслуживающего персонала с позиций предоставления полномочий, ответственности за порученное дело, степени доверия к ним и т. д.

2.2.1 К предположениям о предполагаемых условиях эксплуатации типового объектабудем относить следующие:

— наличие на объекте политики безопасности, определяющей совокупность правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности;

— использование на объекте сертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи;

— отсутствие на объекте электронных устройств для перехвата информации в технических средствах обработки, хранения и передачи информации по каналам связи;

— принятые на объекте организационные и административные меры, технические способы реализации защиты объекта и их элементов должны соответствовать принятым угрозам и характеристикам нарушителей.

2.2.2 К предположениям о физической защите среды безопасности типового объекта будем относить следующие:

— наличие на объекте физических преград несанкционированным действиям нарушителя в отношении объекта и его персонала с целью затруднения (задержки) продвижения нарушителя к объектам защиты на время, необходимое для прибытия сил реагирования;

— разделение территории объекта, как минимум, на три функциональные зоны, доступ в которые должен осуществляться согласно установленным правам доступа.

Зона общего доступа:

— включает здания, территории, помещения, доступ в которые персоналу и посетителям не ограничен;

— доступ в зону осуществляется по одному аутентификационному фактору.

Зона ограниченного доступа:

— включает помещения, доступ в которые разрешен ограниченному составу персонала, а также посетителям объекта по разовым пропускам или в сопровождении персонала объекта;

— доступ в зону осуществляется по двум аутентификационным факторам.

Зона режимного доступа:

— включает специальные помещения объекта, доступ в которые имеют только определенные сотрудники и руководители;

— доступ в зону осуществляется по трем аутентификационным факторам.

Как правило, практическое сопряжение полномочий управ-

ления ресурсами объекта/объектом всегда находиться на стыке нескольких служб, управлений компании. Естественно, что каждый руководитель структурного звена, выполняющего уникальные функции, уже потенциально негативно относиться к вопросу своей подконтрольности со стороны службы безопасности. Часто вопросы передела сфер влияния между отдельными руководителями переходят в проблемы личностной неприязни, что уже гипотетически не позволяет выполнить задачи по консолидации всех заинтересованных структурных подразделений компании в достижении общей цели, связанной с обеспечением гарантированной защиты бизнеса. Выстраивание четких функциональных связей по горизонтали и вертикали с выставлением соответствующих прав доступа — одна из основных задач руководителя службы безопасности компании.

2.2.3 К предположениям относительно администраторов безопасности, пользователей и обслуживающего персонала с позиций предоставления полномочий, ответственности за порученное дело, степени доверия к ним и т. д. в порядке приоритета будем относить следующие:

а) Наличие на объекте руководителей высшего звена управления.

Основная задача руководства объекта — общее управление производственной и административно-хозяйственной деятельностью объекта.

Укрупненная структура:

— директор;

— первый заместитель — начальник службы безопасности;

— заместитель директора — начальник службы автоматизации;

— заместитель директора по производственным вопросам;

— заместитель директора — начальник службы кадров.

Полномочия и степень доверия:

— обладают высшим приоритетом в принятии решений по обеспечению комплексной защиты объекта: остановка функционирования объекта, прием на работу персонала, принятие мер реагирования по инцидентам безопасности на объекте;

— имеют свободный доступ в общую, ограниченную зоны, в режимную зону — при наличии разрешения директора и руководителя службы безопасности.

б) Наличие на объекте службы информационной и инженерно-технической безопасности.

Основная задача подразделения — разработка и реализация политики безопасности, адекватной целям и задачам безопасного функционирования объекта.

Укрупненная структура подразделения:

— руководитель подразделения — разрабатывает и контролирует выполнение политики безопасности объекта;

— администратор безопасности — занимается практической реализацией политики безопасности объекта, администрированием прав доступа;

— аудитор — занимается оценкой текущего состояния по обеспечению комплексной защиты объекта на соответствие требованиям корпоративных, национальных и международных стандартов.

Полномочия и степень доверия:

— обладают высоким приоритетом в принятии решений по обеспечению комплексной защиты объекта: приостановка функционирования объекта, проверка и допуск к работе персонала, проведение разбирательств по инцидентам безопасности на объекте;

— имеют свободный доступ в общую, ограниченную зоны, в режимную зону — при наличии разрешения руководителя службы безопасности.

в) Наличие на объекте службы автоматизации.

Основная задача подразделения — внедрение и эксплуатация систем автоматизации и телекоммуникации.

Укрупненная структура подразделения:

— руководитель подразделения — разрабатывает планы по внедрению и эксплуатации систем автоматизации и телекоммуникаций, контролирует их исполнение;

— администратор систем автоматизации — занимается практическим внедрением и администрированием систем автоматизации и телекоммуникаций;

— супервизор — занимается эксплуатацией систем автоматизации и телекоммуникаций, проведением их оперативного ремонта и восстановления.

Полномочия и степень доверия:

— обладают не высоким приоритетом в принятии решений по обеспечению комплексной защиты объекта: частичная приостановка функционирования систем автоматизации объекта, тестирование персонала, выдача рекомендаций при проведении разбирательств по инцидентам безопасности на объекте;

— имеют свободный доступ в общую зону, в ограниченную зону — при наличии разрешения службы безопасности, в режимную зону — при наличии разрешения руководителя службы безопасности и руководителя подразделения.

г) Наличие на объекте производственных, административно-хозяйственных и др. подразделений.

Основная задача подразделений — обеспечение производственной и административно-хозяйственной деятельностью объекта.

Укрупненная структура подразделения:

— руководитель подразделения;

-специалист подразделения.

Полномочия и степень доверия:

— не обладают приоритетом в принятии решений по обеспечению комплексной защиты объекта: информируют руководство о потенциальных и произошедших инцидентах безопасности;

— имеют доступ в общую зону по разрешению службы безопасности, в ограниченную зону — при наличии разрешения руководителя службы безопасности и руководителя подразделения, в режимную зону — в исключительных случаях при наличии разрешения директора и руководителя службы безопасности.

2.3 Угрозы несанкционированного доступа к типовому объекту.

Проведение любой аналитической работы предполагает введение опорной решетки ценностей. В отношении адекватного реагирования по возникающим инцидентам безопасности можно сказать, что опорной решеткой ценностей является структура сопоставления угроз безопасности к мерам защиты от их деструктивного воздействия. Каждый объект, подлежащий защите, обладает перечнем как типовых, так и уникальных уязвимостей, в основной степени определяемых

функционально-экономической моделью организации процесса функционирования объекта. Классификация и построение опорной структуры: угроза — уязвимость — средство защиты — с учетом специфики объекта является одной из основных задач службы безопасности компании.

При рассмотрении угроз информационной и инженерно-технической безопасности типового объекта необходимо выполнять их анализ с учетом жизненного цикла системы защиты и предъявляемых к ней требований, что в совокупности гарантирует защиту объекта от НСД.

Классификацию угроз можно представить в следующем виде:

1. Угрозы, возникающие при проектировании системы защиты: возможные ошибки проектирования, технологические угрозы.

2. Угрозы, возникающие при классификации и категорировании объекта защиты:

— угрозы в классификации по признаку важности (экономические);

— угрозы в категорировании (структурные).

3. Угрозы, связанные с нарушением порядка внедрения системы защиты:

— угрозы, связанные с нарушением порядка внедрения распределенных корпоративных систем защиты;

— угрозы, связанные с нарушением порядка внедрения локальных систем защиты.

4. Угрозы, связанные с обучением персонала, контролем качества выполняемых работ:

— угрозы, связанные с недостаточной квалификацией персонала;

— угрозы, связанные с недостаточным обучением персонала;

— угрозы в осуществлении контроля качества выполняемых работ.

5. Угрозы, связанные с нарушением безопасности системы: внешние угрозы, внутренние угрозы.

6. Неэффективное реагирование на угрозы безопасности:

— угрозы, связанные с введением неэффективных специальных планов защиты (при точной классификации перечня угроз системе безопасности);

— угрозы, связанные с отсутствием специальных планов защиты (наличие нетиповых угроз/комбинаций угроз системе безопасности).

7. Угрозы, связанные с долгосрочной модернизацией:

— угрозы, связанные с долгосрочной плановой (закладывается из требований статистического уровня угроз/комбинаций угроз и вариантов прогнозных показателей их развития) модернизацией;

— угрозы, связанные с долгосрочной неплановой (закладывается из требований современного уровня угроз/комбинаций угроз, показатели важности которых были оценены ранее неправильно) модернизацией.

8. Угрозы, связанные с текущей модернизацией: ликвидация идентифицированных угроз, ликвидация скрытых угроз.

Задачи по защите типового объекта от НСД.

Практическая реализация методического подхода по обеспечению информационной и инженерно-технической защиты объекта осуществляется через решение перечня формализованных задач. Руководитель службы безопасности компании в первую очередь заинтересован в грамотной постановке таких задач и поиска путей их решения. Финансирование мероприятий по вопросам безопасности также во многом зависит от «прозрачности» преподнесения перечня указанных задач руководству компании.

Задачи по защите объекта от НСД реализуют следующие принципы:

— принцип обязательности формулировки хотя бы одной задачи для противодействия конкретной угрозе;

— принцип однозначного соответствия между формулировками задач безопасности и формулировками угроз, предположений и политик безопасности. Этот принцип предполагает, что из формулировки задачи потенциальный потребитель задания по безопасности мог бы четко уяснить, против какой угрозы она направлена, какое конкретное правило она обеспечивает, какое предположение она покрывает;

— принцип однозначности определения вклада данной задачи в противодействие конкретной угрозе, в обеспечении конкретного правила политики и в покрытии конкретного предположения. Этот принцип означает, что если данная задача будет решена, то должно быть ясно, будет ли обеспечен для организации приемлемый ущерб при реализации угрозы или этот ущерб будет недопустимым.

На основании вышеизложенного можно сформулировать следующий перечень задач по защите объекта от НСД:

1. Провести проектирование системы защиты объекта с учетом всех требований НПА (ТНПА), учитывая максимально возможный уровень взаимодействия управляющих структур. Для проведения проектирования привлечь квалифицированный персонал, имеющий соответствующую профессиональную подготовку и опыт проведения аналогичных работ. Применение вновь разработанных и/или существующих технологий безопасности осуществлять в строгом соответствии с конкретными методическими подходами и технологическими картами.

2. Провести классификацию и категорирование объекта с учетом оценки важности объекта/ресурсов объекта в строгом соответствии с нормами категорирования объектов.

3. Минимизировать цепочки принятия конечного решения по вопросам внедрения системы защиты объекта, а также максимально эффективно использовать опыт и знания квалифицированного персонала.

4. Провести правильную оценку квалификации персонала, обеспечить эффективный контроль за качеством выполняемых работ.

5. Обеспечить своевременное выявление открытых/скрытых уязвимостей в системе безопасности объекта, разработать соответствующие подходы.

6. Обеспечить эффективное реагирование на угрозы безопасности объекта, использующие наличие функциональных уязвимостей в алгоритме его защиты.

7. Разработать и/или внедрить механизмы реагирования на появление новых прогнозируемых угроз системе безопасности объекта.

8. Разработать и/или внедрить механизмы реагирования на появление идентифицированных угроз, ликвидация скрытых угроз системе безопасности объекта. ■