УДК 654.924

ПОДХОД К ОЦЕНКЕ ВЕРОЯТНОСТИ ПРЕСЕЧЕНИЯ НЕСАНКЦИОНИРОВАННЫХ ДЕЙСТВИЙ В ОБЪЕДИНЕННОЙ СИСТЕМЕ БЕЗОПАСНОСТИ

Владимир Волхонский
Санкт-Петербургский Государственный университет аэрокосмического приборостроения

Аннотация: **Анализируются состав объединенной системы безопасности, зоны охраны и последовательность событий при проникновении на охраняемый объект. Рассматриваются составляющие временных параметров, предлагается метод оценки вероятности пресечения проникновения на охраняемый объект.**
Summary: **Analysis of general security system, security zones and event sequence for intrusion process. Based on time intervals of this process, estimation method of catching intruder probability is offered.**
Ключевые слова: **Безопасность, зоны, вероятность, пресечение, проникновение.**

Практика показывает, что применение отдельных систем или подсистем обеспечения информационной безопасности во многих случаях является недостаточным [1]. Полное решение проблемы возможно лишь на основе интеграции всей объединенной системы обеспечения безопасности в целом, включающей в себя техническое, ресурсное и правовое обеспечение (ТО, РО, ПО), а кроме этого и организацию деятельности службы (ОДС). При этом, техническое обеспечение предполагает использование аппаратных и программных средств. Проанализируем, на основе структуры объединенной системы информационной безопасности (ОСБ), ее временные параметры, определяющие возможность оценки такой важной характеристики, как вероятность пресечения несанкционированных действий на объекте, т.е. выполнения основной функции ОСБ.

I Структура системы обеспечения безопасности

Техническое обеспечение безопасности объекта включает в себя собственно технические средства обеспечения безопасности (ТСОБ) и средства доставки (автотранспорт). Рассмотрим подробнее структуру и основные подсистемы технических средств обеспечения безопасности, представленную на рисунке 1, прямо или косвенно решающие задачи обеспечения информационной безопасности.

Рисунок 1 – Структура и основные подсистемы ТСОБ

Конкретные задачи и условия функционирования ТСОБ зависят от объекта защиты, на котором в первую очередь необходимо определить последовательные зоны охраны с одновременным выявлением угроз по каждой конкретной зоне (рисунок 2).

К первой зоне охраны относится периметр территории, на которой находится охраняемый объект. В первой зоне могут использоваться средства инженерной защиты (СИЗ) такие как: различного вида заграждения, заборы; средства телевизионного наблюдения (СТВН); средства охраны периметра (активные и пассивные), а также и физическая охрана (ФО).

Вторая зона охраны включает в себя территорию, на которой находится охраняемый объект. При защите данной зоны используется комплекс мероприятий, состоящий в использовании СТВН и соответствующей группы технических средств охранной сигнализации (ТС ОПС).

Рисунок 2 – Зоны охраны

Третья зона охраны, это периметр объекта - охраняемого здания или помещения. Эта зона контролируется СТВН, ТС ОПС и ИСЗ.

Четвертая зона - внутренние объемы объекта. С организационной точки зрения в четвертой зоне можно выделить следующие дополнительные зоны. Зоны свободного доступа (сотрудников, клиентов и т.п.). Зоны ограниченного по времени доступа, например, сотрудников - режимом работы предприятия. Зоны ограниченного по уровню приоритета доступа, к примеру, сотрудников, имеющих право на посещение помещений с концентрацией материальных и информационных ресурсов, залы для заседаний, кабинеты совещаний и т п. Специальные зоны, такие как помещения руководства объекта и охраны. Зоны непосредственного сосредоточения и хранения материальных ценностей и информации. Эти зоны должны контролироваться ТС ОПС, средствами контроля доступа (СКД), СТВН, совместно со средствами защиты информации (СЗИ), ФО.

Пятая зона - отдельные предметы. Например, компьютеры, сейфы, места хранения документации и так далее. Для защиты используется соответствующая группа ТС ОПС.

Шестая зона - собственно система безопасности. В первую очередь включает в себя защиту технических и программных средств обеспечения безопасности. Угрозы - несанкционированный доступ к элементам системы безопасности с целью либо полного вывода из строя, либо блокировки отдельных элементов, делающей невозможной выполнение ими основных функций при внешнем сохранении работоспособности.

Любая из рассмотренных зон в зависимости от значимости объекта или его элементов, контролируемых данной зоной, может включать в себя несколько рубежей охраны.

II Анализ временных параметров системы

Учтем, что в составе ОСБ имеются средства обнаружения несанкционированных действий, система передачи извещений, пункт централизованной или автономной охраны (ПЦО или ПАО) с соответствующими службами и группами задержания (ГЗ). Сразу оговорим, что здесь не рассматриваются вопросы, связанные с процессом непосредственного задержания. Оценивается только вероятность “встречи” сотрудников охраны с преступниками.

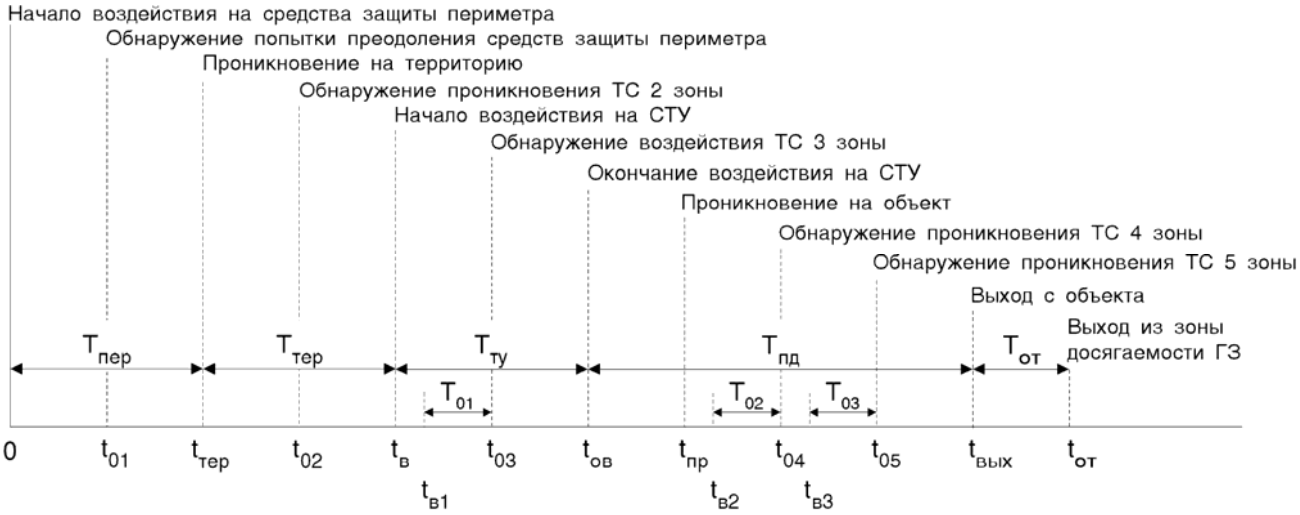

Рисунок 3 – Последовательность событий при проникновении на объект

Предположим, что система безопасности имеет пять зон охраны, рассмотренных выше. Проанализируем последовательность событий во времени для различных сценариев развития процесса проникновения на охраняемый объект и реакции различных элементов системы безопасности. Диаграмма, приведенная на рисунке 3, иллюстрирует возможную последовательность событий при проникновении на охраняемый объект. Будем обозначать малой буквой t моменты времени, а большой Т - длительности. За начало отсчета возьмем момент начала воздействия на средства охраны периметра.

Соответственно реакция системы сигнализации и действия службы охраны от начала воздействия $t_{вi}$ на контролируемый параметр средств обнаружения i-й зоны могут быть проиллюстрированы на рисунке 4. Под контролируемым параметром будем понимать параметр физического процесса (вибрация, открывание, разбивание, движение, ...), регистрация изменения которого лежит в основе принципа действия устройства обнаружения. Возможная задержка входа/выхода при снятии и постановке объекта на охрану определяется тактикой использования объектового оборудования [3]. Процесс передачи извещения на интервале времени $T_{СПИ}$ включает взаимодействие объектового оборудования с объектовым устройством СПИ, процедуру установления связи, передачу извещения, обработку извещения ПЦН и реакцию дежурного пульта. Задержка $T_{ЗГЗ}$ на оповещение группы задержания может быть вызвана ожиданием процедуры подтверждения пользователем дежурному пульта санкционированности действий при нарушении зоны входа/выхода. При проникновении через зоны тревоги в режиме охраны или 24-часовые задержки входа/выхода и на оповещение ГЗ должны быть равны нулю. Ясно, что при выборе ТС обнаружения и мест их установки, необходимо стремиться к минимизации интервалов между началом несанкционированных действий (или попыткой проникновения) и началом воздействия на контролируемый параметр технических средств обнаружения i-й зоны. Например, желательно обеспечить контроль всего объема помещения, а не только наиболее уязвимых мест. Кроме того, очевидно, что необходимо сводить к минимуму и значения T_{Oi} . Последнее достигается главным образом правильными выбором, установкой и настройкой устройств обнаружения.

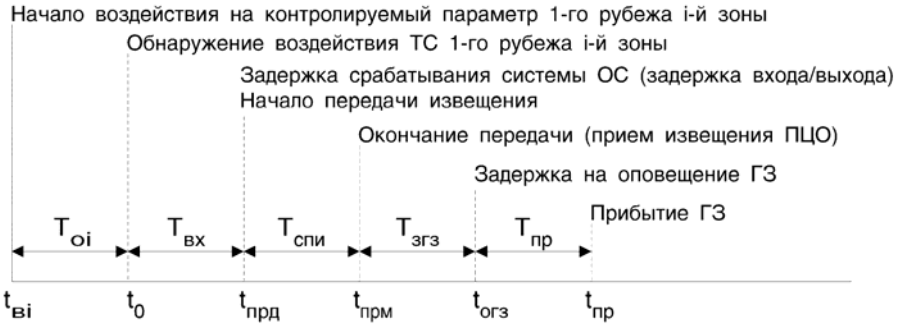

Рисунок 4 – Последовательность действий системы и службы охраны

Общая продолжительность несанкционированных действий, позволяющая оценить вероятность его пресечения, будет определяться выражением

$$T_{нп} = T_{пер} + T_{тер} + T_{ту} + T_{пд} + T_{от} , \quad (1)$$

где $T_{ПЕР}$ - продолжительность преодоления средств охраны периметра, $T_{ТЕР}$ - продолжительность преодоления прилегающей к объекту территории, $T_{ТУ}$ - продолжительность преодоления средств технической укрепленности, $T_{ПД}$ – длительность совершения противоправных действий на объекте, $T_{ОТ}$ – продолжительность отхода за пределы зоны досягаемости группы задержания (ГЗ). Последний параметр целесообразно учесть при оценке вероятности пресечения противоправных действий, так как даже покинув объект, преступники могут быть обнаружены и задержаны нарядом ГЗ вблизи охраняемого объекта.

Задержка прибытия ГЗ складывается из нескольких составляющих.

$$T_з = T_о + T_{зад} + T_{спи} + T_{згз} + T_{пр} . \quad (2)$$

В последнем выражении $T_О$ – временной интервал, необходимый для обнаружения проникновения техническими средствами обнаружения первого рубежа i-й зоны от момента начала воздействия на СТУ, $T_{ЗАД}$ –задержка на

формирование сигнала тревоги системой ОС при проникновении через зоны входа/выхода [3], $T_{СПИ}$ - длительность передачи извещения СПИ, $T_{ЗГЗ}$ - задержка на оповещение ГЗ, $T_{ПР}$ – продолжительность прибытия ГЗ.

III Оценка вероятности пресечения несанкционированных действий

Обозначим $p(t_{нп})$ – плотность вероятности продолжительности несанкционированных действий $p(t_З)$ – плотность вероятности задержки прибытия ГЗ (рисунок 5). Под переменной $t_{нп}$ будем понимать разность $t_{нп} = t_{от} - t_{oi}$ момента $t_{от}$ выхода из зоны досягаемости ГЗ и момента t_{oi} обнаружения. Плотность вероятности $p(t_З)$ может быть оценена на основе статистических данных о задержке прибытия ГЗ на объект по тревоге, а $p(t_{нп})$ на основе статистики и экспертных оценок.

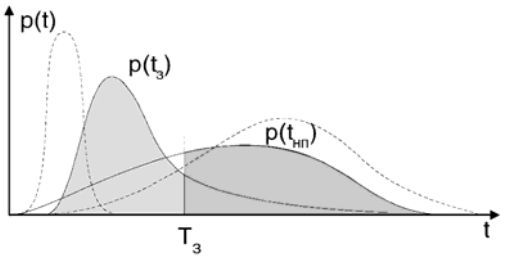

Рисунок 5 - Плотности вероятности длительностей $t_{нп}$ и $t_З$.

Рассмотрим систему двух случайных величин ($t_{нп}$, $t_З$) с совместной плотностью вероятности $p(t_{нп}$, $t_З$) (рис. 5). Тогда вероятность своевременного прибытия ГЗ и пресечения несанкционированных действий будет определяться выражением

$$P_{пп} = \int_{Tз}^{\infty} \int_{0}^{Tз} p(t_{нп}, t_З) dt_{нп} dt_З . \qquad \textit{(3)}$$

В предположении, справедливом для многих практических приложений, что действия преступников и службы охраны независимы, выражение упростится и вероятность $P_{ПП}$ определится формулой

$$P_{пп} = P(t_{нп} \geq T_З) P(t_З \leq T_З) . \qquad \textit{(4)}$$

В последнем выражении обозначены, соответственно, $P_{НП}=P(t_{нп} \geq T_З)$ вероятность того, что длительность несанкционированного проникновения $t_{нп}$ больше задержки $T_З$ прибытия наряда ГЗ и $P_З=P(t_З \leq T_З)$ вероятность того, что задержка $t_З$ прибытия ГЗ меньше интервал времени $T_З$.

Из полученных выражений (3) и (4) и рис. 5 видно, что для увеличения вероятности $P_{ПП}$ необходимо стремиться к увеличению $P_З$ и $P_{НП}$. Увеличение первой составляющей происходит с уменьшением среднего значения $M[t_З]$ и дисперсии $D[t_З]$ задержки прибытия ГЗ. Каким образом это может достигаться? Для этого проанализируем параметры, входящие в выражение (2).

- $T_{СПИ}$ – технический параметр СПИ. Может составлять от долей до единиц секунд в большинстве СПИ, используемых вневедомственной охраной, и до десятков секунд в других системах, к примеру, использующих метод автодозвона.
- Математическое ожидание $M[t_З]$ случайной величины $t_З$ будет иметь составляющую $M_0= T_{ЗАД} + T_{ЗГЗ}$. Эти задержки определяются особенностями функционирования системы ОС и тактикой работы ПЦО. Ясно, что эти параметры должны быть минимизированы в разумных пределах (чрезмерное уменьшение может привести к росту вероятности ложных тревог).
- Значения T_{Oi} могут составлять от долей до десятков секунд. Например, в соответствии с ГОСТ Р 50777-95 для пассивных инфракрасных извещателей при перемещении стандартной цели (чувствительности) на 3 м и минимальной скорости движения 0,3 м/с промежуток времени, необходимый для обнаружения, может иметь величину до 10 с. При этом не учитывается отличие реальной цели от стандартной и условия на объекте, что может еще увеличить это значение.

Для увеличения $P_{НП}$ необходимо увеличивать среднее значение $M[t_{нп}]$ и уменьшать дисперсию $D[t_{нп}]$. Пути достижения этого достаточно подробно рассмотрены в [2] и заключаются, в основном, в усилении средств технической укрепленности. То есть в косвенном воздействии на преступника, вынуждающем его затратить больше времени на преодолении этих средств.

Использование нескольких рубежей охраны в каждой зоне позволяет существенно повысить вероятность обнаружения несанкционированных действий. Пусть P_1 , P_2 , P_3 – вероятности обнаружения проникновения ТС охраны соответственно для 1, 2 и 3 рубежей через интервал времени $T_{вi}$ после начала воздействия на контролируемый параметр i-го рубежа охраны. Вполне обоснованно можно предположить, что разные рубежи охраны используют извещатели с разным физическим принципом действия. Тогда можно считать, что события обнаружения проникновения извещателями каждого рубежа независимы и совместны. В этом случае вероятность обнаружения проникновения хотя бы одним рубежом системы сигнализации определяется известным выражением $P=P_1+P_2+P_3- P_1P_2- P_1P_3- P_2P_3+ P_1P_2P_3$. К примеру, при вероятности обнаружения каждым рубежом $P_i=0.8$, вероятность обнаружения системой сигнализации в целом составит 0,992. Однако, очевидно, что промежуток времени с момента начала воздействия на СТУ до обнаружения проникновения может заметно возрасти при пропуске нарушителя первым или первым и вторым рубежами. Это связано, во-первых, с более поздним воздействием на контролируемый параметр следующего рубежа и, во-вторых, с отличием во времени, необходимом для обнаружения проникновения извещателями с разным физическим принципом действия.

Таким образом наиболее эффективное решение задачи разработки системы защиты информации воз-можно лишь на основе интеграции объединенной системы обеспечения безопасности в целом, с использованием всех технических средств. Конкретные особенности, состав и условия функционирования ТСОБ будут зависеть от выявленных угроз. Целесообразно использование многозонной многорубежной охраны. Предложенный спо-соб позволяет получить оценку вероятности пресечения несанкционированных действий на охраняемом объекте.

Литература: 1. В.Волхонский, А.Засыпкин, В.Коротких. Структура технических средств обеспечения безопасности. БДИ //Безопасность, достоверность, информация. СПб., 1999, №3 ,С.18-20. 2. Н.В.Линев, А.А.Никитин, А.В.Климов. Раннее обнаружение несанкционированного проникновения //Системы безопасности, М., № 27, 1999, С.24 - 31. 3. В.В.Волхонский. Устройства охранной сигнализации. - СПб.: Экополис и культура, 1999. - 271 с.

УДК 659.2.002

КОНЦЕПЦИИ ЗАЩИТЫ ОТДЕЛЬНЫХ ОБЪЕКТОВ — НЕОБХОДИМАЯ СОСТАВНАЯ ЧАСТЬ НОРМАТИВНОЙ БАЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Виктор Маслак

Казенное предприятие "Харьковское конструкторское бюро по машиностроению имени А.А. Морозова"

Анотація: **В доповіді викладений один із шляхів удосконалення нормативної бази інформаційної безпеки держави. Обгрунтована необхідність розробки концепцій захисту окремих об′єктів, які є носіями таємної інформації.**

Summari: **The report expounds one of the possible ways of perfecting the normative base of informational security of the state, substantiates the necessity of development of conceptions of protection of separate objects which contain secret information.**

Ключевые слова: **концепция, информация, защита, объект.**

I Вступление

Со времени принятия Закона Украины "О государственной тайне" и создания Госкомсекретов Украины Указами Президента и постановлениями Кабинета Министров Украины утверждено и введено в действие много нормативно-правовых актов, которые сегодня составляют основу нормативной базы, обеспечивающей информационную безопасность государства. В то же время вряд ли кто возьмется определить исчерпывающий перечень нормативных документов, которые смогли бы в полной мере охватить все проблемы, связанные с охраной информации ограниченного доступа и прежде всего государственной тайны. Создание необходимой