Метод определения периодичности обновления квалифицирующих признаков попыток вторжений при информационном обмене с робототехническим комплексом

С. А. Матвеев [1], Д. А. Лесняк [2]
Военно-космическая академия имени А.Ф. Можайского
[1] serg15332m@yandex.ru, [2] denislesnyk@mail.ru

***Аннотация*. В целях обеспечения контроля защищенности радиоканала передачи информации с робототехническим комплексом рассмотрена возможность применения многоуровневой системы обнаружения вторжений. Предложен метод определения периодичности обновления квалифицирующих признаков попыток вторжений нарушителем при информационном обмене с роботехническим комплексом.**

Ключевые слова: многоуровневая система обнаружения вторжений; робототехнический комплекс; квалифицирующий признак; защищённости информационного обмена

I. Информационный обмен с робототехническим комплексам

В настоящее время наблюдается бурный рост робототехнических комплексов, которые находят широкое применение в ключевых областях человеческой деятельности. Их востребованность обусловлена высокой производительностью, качеством, экономическими затратами и высокими требованиями к качеству их выполнения. Информационный обмен с робототехническими комплексами (РК), в большинстве случаев, ведется по радиоканалам связи [1], в связи с невысокими экономическими затратами, простотой развертывания и удобством использования. Однако, наличие пространственной электромагнитной доступности, свойственной всем беспроводным каналам связи, создает благоприятные условия для осуществления деструктивных воздействий нарушителя к циркулируемой в ней информации [2]. Таким образом, к радиоканалам связи предъявляются высокие требования по обеспечению информационной безопасности.

Для обеспечения высокого уровня защищенности радиоканала связи необходимо применения многоуровневой систему обнаружения вторжений (СОВ). Состав и количество уровневой СОВ определяется, исходя из ожидаемых угроз, целей потенциального нарушителя и требований к достижению определенного уровня защищенности информационного обмена [3, 4].

Каждому уровню функционирования СОВ соответствует свой квалифицирующий признак (КП) попыток вторжений в радиоканал информационного обмена с РК. Элементами каждого уровня СОВ РК являются логические блоки сопоставления текущего условия информационного обмена с альманахом загруженных КП, требующего периодического обновления в условиях попыток вторжений в радиоканал связи со стороны нарушителя.

II. Метод определения периодичности обновления квалифицирующих признаков попыток вторжений при информационном обмене с робототехническим комплексом

В условиях информационного противоборства объективным свойством защищенности является ее постепенное снижение при отсутствии периодического обновления КП попыток вторжений многоуровневой СОВ [4]. При перехвате передаваемой по радиоканалу информации, нарушитель накапливает данные об используемых методах передачи, что приводит к снижению уровня защищенности и увеличению вероятности вторжения.

Принцип поддержания требуемого уровня защищенности информационного обмена с РК в условиях деструктивных воздействий нарушителя представлен на рис. 1.

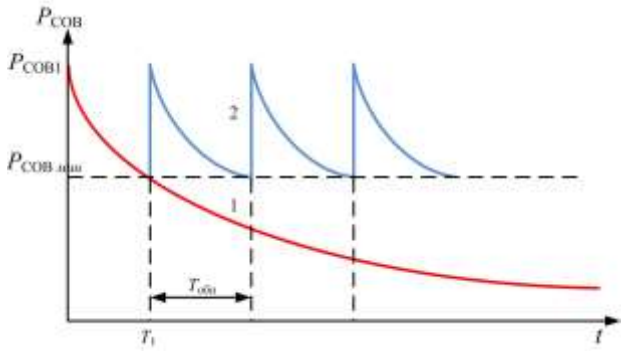

Рис. 1. Изменение во времени вероятности обеспечения информационной безопасности в отсутствие и при наличии периодического обновления квалифицирующих признаков многоуровневой СОВ

Данный принцип соответствует подходу к анализу информационной безопасности с использованием теории надежности [5, 6, 7]. Кривая 1 соответствует снижению с течением времени t вероятность правильного функционирования многоуровневой СОВ $P_{СОВ}$ без обновления КП попыток вторжений, кривая 2 соответствует поддержанию вероятности правильного функционирования многоуровневой СОВ не ниже минимально допустимой $P_{СОВмин}$. Чтобы гарантировать требуемый уровень информационной безопасности, механизм многоуровневой СОВ должен функционировать так, чтобы необходимые обновления КП попыток вторжений проводились через определенный интервал времени $T_{обн}$, выбираемый исходя из допустимого снижения вероятности обеспечения информационной безопасности при правильном функционировании многоуровневой СОВ [6, 7].

В случае, когда поддержание уровня защищенности информационного обмена с течением времени не осуществляется, даже при начальном полностью защищенном состоянии системы ($P_{СОВ}(0)=P_{СОВ1}=1$) через интервал времени T_1 вероятность достигнет минимально допустимое значение $P_{СОВмин}$ и будет продолжать снижаться [6, 7]. Характер изменения (снижения) вероятности $P_{СОВ}$ от времени t будет определяться темпами ведения нарушителем анализа деятельности защищающейся стороны.

Изменение защищенности на заданном интервале времени соответствует экспоненциальному закону распределения вероятностей преодоления многоуровневой СОВ потенциальным нарушителем, как наименее благоприятному с точки зрения обеспечения требуемого уровня защищенности информационного обмена и приводящего к наиболее жестким требованиям к периодичности обновления КП попыток вторжений соответствующих уровней СОВ T, удовлетворяющей условию $P_{СОВ}(T) \geq P_{СОВмин}$ [7].

При экспоненциальном законе распределение вероятности преодоления многоуровневой СОВ нарушителем определяется выражением (1).

$$w_{нап}(t) = \frac{1}{T_{нап}} \exp\left(-\frac{t}{T_{нап}}\right) \qquad (1)$$

где $T_{нап}$ – среднее значение времени преодоления нарушителем уровней СОВ.

Тогда вероятность правильного функционирования многоуровневой СОВ $P_{СОВ}(t)$ определяется выражением (2).

$$P_{СОВ}(t) = \exp\left(-\frac{t}{T_{нап}}\right) \qquad (2)$$

Для выполнения требования вида $P_{СОВ}(T) \geq P_{СОВзад}$ при периодическом обновлении КП попыток вторжений многоуровневой СОВ с интервалом времени $T_{обн}$, что соответствует закону распределения вероятностей обеспечения обнаружения вторжений $w_{ОВ}(t) = \delta\left(t - T_{ОБН}\right)$, подставив в выражение (2) $t=T_{обн}$ и $P_{СОВ}(T_{обн})=P_{СОВ\ доп}$. В результате получаем:

$$T_{обн} = -T_{нап} \ln P_{СОВдоп} \qquad (3)$$

Вероятность ошибочного функционирования многоуровневой СОВ величина $1-P_{СОВ}$ должна иметь порядок 10^{-9}–10^{-12} [8], что определяется вероятностью прохождения ложных информационных сообщений, а вероятность $P_{СОВ}$ должна быть близка к 1, экспоненциальную зависимость $P_{СОВ}(t)$, определяемую выражением (2), можно заменить линейной (4):

$$P_{СОВ}(t) = \exp\left(-\frac{t}{T_{нап}}\right) \approx 1 - \frac{t}{T_{нап}} \qquad (4)$$

На рис. 2 приведены зависимость $P_{СОВ}(t/T_{нап})$, соответствующая экспоненциальной плотности распределения вероятностей преодоления многоуровневой СОВ (кривая 1), и ее линейная аппроксимация (кривая 2).

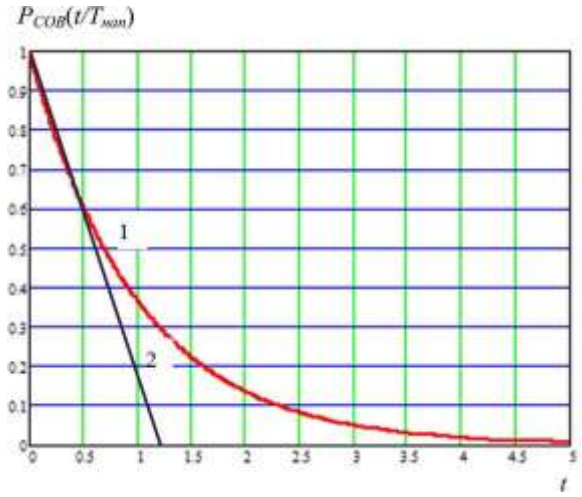

Рис. 2. Плотность распределения вероятностей преодоления нарушителем многоуровневой СОВ

На рис. 3 приведены зависимости отношения $T_{обн}/T_{нап}$ от вероятности $P_{СОВ\ доп}$.

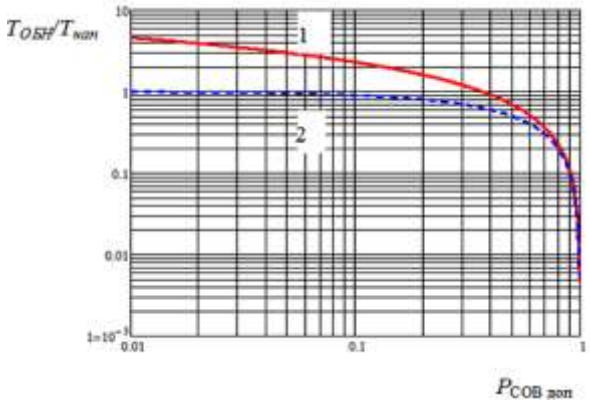

Рис. 3. Определение требуемой периодичности обновления квалифицирующих признаков попыток вторжений многоуровневой СОВ при информационном обмене с робототехническим комплексом

Кривая 1 соответствует определению требуемой периодичности обновления КП многоуровневой СОВ при информационном обмене с РК с интервалом $T_{обн}$ в соответствии с выражением (2), кривая 2 – в соответствии с выражением (3).

Приведенные зависимости показывают, что в интересующей области значений вероятности $P_{\text{СОВ}}$ для определения периодичности обновления КП попыток вторжения многоуровневой СОВ $T_{\text{обн}}$ может быть использована линейная аппроксимация зависимости $P_{\text{СОВ}}(t/T_{\text{нап}})$ и выражение (5).

Тогда требуемая при заданной вероятности правильного функционирования $P_{\text{СОВ доп}}$ периодичность обновления КП вторжений многоуровневой СОВ определяется выражением (5):

$$T_{обн} = T_{нап}\left(1 - P_{СОВдоп}\right) \quad (5)$$

Необходимыми исходными данными для определения величины $T_{\text{обн}}$ являются вероятность правильного функционирования многоуровневой СОВ $P_{\text{СОВ доп}}$ и ожидаемое среднее значение времени преодоления уровней СОВ нарушителем $T_{\text{нап}}$.

Полагая $P_{\text{СОВ доп}} = (1–10^{-12})$, по формуле (5) находим соответствующие значения требуемой периодичности обновления КП многоуровневой СОВ: $T_{\text{обн}}$ =1–1,5 месяцев при работе в штатном режиме, $T_{\text{обн}}$ = (10–15) дней в периоды активации нарушителя.

Таким образом, получение информации нарушителем, при передаче по радиоканалам информационного обмена с РК, может привести к снижению его целевого эффекта применения.

В условиях информационного противоборства предлагаемый подход к построению многоуровневой СОВ позволяет предотвратить попытки вторжения нарушителя к радиоканалу связи при информационном обмене с РК, а представленный метод периодического обновления КП попыток вторжения позволяет поддерживать требуемый уровень защищённости информационного обмена с робототехническим комплексом.

Список литературы

[1] Спутниковая связь и вещание. Справ. / Под ред. Л.Я Кантора. М.: Радио и связь, 1997. 528 с.

[2] Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая линия–Телеком, 2004. 280 с.

[3] Мальцев Г.Н., Матвеев С.А. Математические модели процесса преодоления нарушителем многоуровневой системы защиты информации // Труды Военно-космической академии имени А.Ф. Можайского 2020. №673. С.126–136

[4] Свидетельство о государственной регистрации ПЭВМ № 2020662710 Программа для моделирования бортовой системы обнаружения вторжений в радиоканал управления робототехническим комплексом / С.А. Матвеев, Г.Н. Мальцев, Д.А. Лесняк. М.:ФИПС, 2020.

[5] Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. М.: РадиоСофт, 2010. 232 с.

[6] Мальцев Г.Н., Лесняк Д.А. Применение стратегий поддержания защищенности в информационных системах // Информационно-управляющие системы. 2017. №3 (88). С.67–74.

[7] Мальцев Г.Н., Панкратов А.В., Лесняк Д.А. Исследование вероятностных характеристик изменения защищенности информационной системы от несанкционированного доступа нарушителей // Информационно-управляющие системы. 2015. №1. С.50–59.

[8] Комашинский В.И., Максимов А.В. Системы подвижной радиосвязи с пакетной передачей информации. Основы моделирования. М.: Горячая линия–Телеком, 2007. 176 с.