ОСОБЕННОСТИ АНАЛИЗА РИСКОВ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ ПРИ СОЗДАНИИ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ

***Казарин Олег Викторович**, доктор технических наук, старший научный сотрудник, ведущий научный сотрудник Института проблем информационной безопасности МГУ им.Ломоносова, г. Москва*
E-mail: okaz2005@yandex.ru
***Репин Максим Михайлович**, аспирант МГТУ им. Н.Э.Баумана, г. Москва*

В работе рассмотрена задача анализа рисков утечки конфиденциальной информации по техническим каналам на этапах разработки и испытаний радиоэлектронных средств.

Представлены модель возникновения нарушений и угроз на объекте защиты и процедура анализа рисков утечки конфиденциальной информации и оценки экономической обоснованности построения системы защиты информации от утечки по техническим каналам на данных этапах жизненного цикла таких средств.

***Ключевые слова**: радиоэлектронное средство, технические каналы утечки информации, анализ рисков.*

THE FEATURES OF THE RISK ANALYSIS OF CONFIDENTIAL INFORMATION LEAK THROUGH TECHNICAL CHANNELS FOR CREATING RADIO-ELECTRONIC EQUIPMENT

***Oleg Kazarin**, Doctor of Science (Comp), Associate Professor, Senior researcher at the Institute of problems of information safety of Lomonosov Moscow State University, Moscow*
E-mail: okaz2005@yandex.ru
***Maksim Repin**, graduate student of Bauman MSTU, Moscow*

The paper deals with the task of analyzing the risk of leakage of confidential information through technical channels on the stages of development and testing of electronic equipment.

The model of occurrence of infringements and threats on object of protection and procedure of the analysis of risks of leak of the confidential information and an estimation of economic validity of construction of system of protection of the information from leak on technical channels at the given stages of life cycle of such means are presented.

***Keywords**: radio-electronic equipment, the technical channels of information leakage, risk analysis.*

Введение

В настоящее время радиоэлектронные средства (РЭС) составляют основу систем управления различными видами техники во всех областях жизнедеятельности человека. Разработка подобных устройств связана с поиском и реализацией инновационных решений и является одной из самых наукоемких областей высокотехнологичного производства. В связи с этим, планирование, обеспечение и контроль работ по защите инфор-

мации о разрабатываемых средствах является важной задачей на всех этапах опытно-конструкторских работ и на этапе испытаний опытного образца, в частности.

Для построения систем защиты информации при проведении разработки РЭС обычно используется подход, основанный на положениях нормативно-методических документов, разработанных регуляторами в области технической защиты информации, согласно которым, в зависимости от типов защищаемого объекта применяется рекомендованный перечень организационных и технических мер защиты. Данный подход имеет существенный недостаток, заключающийся в том, что он не учитывает специфические особенности объекта защиты и не основан на проведении анализа рисков информационной безопасности, актуальных для объекта защиты.

1. Типовой порядок и содержание работ по защите информации на этапах разработки и испытаний образца РЭС

Рассмотрим типовой порядок и содержание работ по защите информации на этапах разработки и испытаний образца РЭС.

Стадии разработки образца РЭС обычно подразделяется на ряд подэтапов [1]:

- этап эскизного проектирования;
- этап технического проектирования;
- этап разработки рабочей документации для изготовления опытного образца и изготовление опытного образца;
- этап испытаний опытного образца РЭС;
- этап корректировки рабочей документации и доработки опытного образца РЭС по результатам испытаний.

На данных подэтапах проводятся следующие мероприятия по защите информации [2, 9]:

- определение целей защиты информации об образце РЭС;
- определение опасных видов угроз для каждой стадии жизненного цикла образца РЭС;
- определение перечня охраняемых сведений об образце РЭС;
- разработка перечня мероприятий по защите информации об образце РЭС и контролю их эффективности;
- разработка требований к средствам, мерам по защите информации и контролю эффективности защиты информации;
- проведение оценки реализуемости требований по защите информации к конструкции образца РЭС;
- определение состава средств защите информации и контроля эффективности защите информации;
- реализация мер защиты.

Результаты, получаемые от проведения данных мероприятий, носят субъективный характер, так как основаны только на экспертных оценках без проведения работы по анализу актуальных угроз утечки конфиденциальной информации и ее рисков.

2. Задача поиска радиосигнала и распознавания его источника, решаемая при проведении разведки РЭС

В общей постановке задача выявления каналов утечки информации и оценки эффективности существующей системы защиты информации при разработке и испытаниях образца РЭС может рассматриваться как задача поиска радиосигнала и распознавания его источника, решаемая при проведении разведки РЭС [3-5].

Разработка, испытание, изготовление и эксплуатация средств и систем РЭС связаны с излучением электромагнитных волн радиодиапазона, которые могут нести информацию о назначении и характеристиках создаваемых и эксплуатируемых средствах и системах. Перехват и анализ радиоизлучений дает возможность противнику получать сведения о новых разработках радиоэлектронных устройств, их назначении и характеристиках.

Для рассматриваемого случая, из всего спектра существующих видов нарушений требований (норм) эффективности технической защиты информации актуальными являются [6-8]:

- превышение допустимого уровня радиоизлучений, модулируемых информационным сигналом, возникающих в различных генераторах в РЭС и вспомогательных средствах или возникающих при наличии паразитной генерации в узлах и элементах технических средств;
- превышение допустимого уровня побочных электромагнитных излучений от РЭС и вспомогательных средств;
- наличие радиоизлучений, обусловленных воздействием на РЭС высокочастотных сигналов;
- наличие радиоизлучений, используемых в канале передачи данных технических средств разведки;
- наличие радиоизлучений от несанкционированно применяемых на территории ОЗ средств радиосвязи.

3. Модель возникновения нарушений установленных требований эффективности защиты информации на объекте

Для проведения обоснованной постановки задачи необходимо сформировать модель возникновения нарушений установленных требований (норм) эффективности защиты информации на объекте (угроз).

Необходимо отметить, что причины возникновения угроз в различных случаях, как правило, различны. При этом, моменты их возникновения являются взаимонезависимыми. Пусть N – показатель частоты реализации угрозы одного типа. Для определения данного показателя необходимо проанализировать характеристики нарушений на объекте o и действия, предпринимаемые противником для перехвата данных. Под объектом o понимаются объекты, на которые возможно проведение атаки (объект РЭС, контрольно-измерительная аппаратура, различные вспомогательные устройства, тренажеры, имитаторы, стенды и т.д.).

Далее определим:

$N = F(T_{отн}; \lambda_н; M(d,i))$,

где:

– i – противник, использующий определенные средства перехвата информации;

– d – охраняемые сведения об объекте РЭС или иная конфиденциальная информация;

– $T_{отн}$ – показатель относительного времени наличия нарушения на объекте;

– $\lambda_н$ – интенсивность потока нарушений;

– $M(d,i)$ – способ реализации угрозы противником, включающий способ перехвата (угрозу) и способ использования перехваченных данных:

$M(d,i) = (Mu(d,i); Mr(d,i))$,

где:

– $Mu(d,i)$ – способ перехвата информации (перехват осуществляется с объекта o с помощью действий $u(o)$);

– $Mr(d,i)$ – способ использований противником перехваченных данных с помощью действий $u(d)$.

Важным фактором, анализ которого необходимо проводить при построении системы защиты информации является число инцидентов утечки конфиденциальной информации с объектов, аналогичных или близких по характеристикам к исследуемому объекту защиты. Пусть:

– $e(M)$ – инцидент в области безопасности;

– $e(M) = (e(Mu); e(Mr))$;

– $N(M)$=$N(e(M))$ – количество инцидентов с использованием способа реализации угрозы, зафиксированных в статистических данных;

– $N(Mu), N(Mr)$ – количество инцидентов с использованием способа перехвата информации и способа использования информации:

$N(Mu) = Ns(Mu) + Nf(Mu), N(Mr) = Ns(Mr) + Nf(Mr)$,

где:

– $Ns(Mu), Ns(Mr)$ – количество успешных атак с использованием способа перехвата информации и способа использования информации соответственно;

– $Nf(Mu), Nf(Mr)$ – количество предотвращенных атак с использованием способа доступа и способа использования информации соответственно.

$T_{отн} = \frac{T_{сум}}{T_{ои.сум}}$,

где:

$T_{сум}$ – суммарное время наличия нарушения на объекте;

$T_{ои.сум}$ – суммарное время обработки информации на объекте.

$T_{сум} = \sum_{i=1}^{k} t_{y,i}$,

где $t_{y,i}$ – продолжительность обработки защищаемой информации от момента возникновения нарушения до его устранения.

$\lambda_н = \frac{T_{ои.сум}}{T_o}$,

где T_o – среднее значение временного интервала между нарушениями (среднее число нарушений на исследуемом интервале времени).

Таким образом, параметрами модели возникновения нарушений и угроз, характеризующими их, являются характеристики, определяющие время наличия нарушений и угроз на объекте защиты, интенсивность возникновения нарушений и статистические данные, способы перехвата конфиденциальной информации.

4. Процедура анализа рисков

4.1. Установленные обозначения

Для описания процедуры введем следующие условные обозначения:

– $k(d), k(o)$ – мера защиты, применяемая к охраняемым сведениям или объектам соответственно;

– T – время проведения испытания объекта РЭС (время функционирования СЗИ);

– $G(M)$ – экспертная оценка выгоды, получаемой противником от реализации угрозы;

– $V(M)$ – оценка стоимости для противника реализации угрозы;

– $O(d,i)$ – экспертная оценка возможных

финансовых потерь противником i, получившим и реализующим сведения d, вследствие контрдействий владельца информации и применения им средств противодействия;

– R_o – вероятность обнаружения сигнала объекта РЭС или окружения;

– $R(M)$ – оценка вероятности реализации угрозы способом М. Оценка вероятности реализации угрозы рассчитывается на основании статистики инцидентов и расчета вероятности перехвата и раскрытия охраняемых сведений;

– $R^1(M)$ – компонента вероятности, рассчитанная на основании статистики инцидентов, рассчитывается как вероятность выполнения двух совместных событий: получения доступа и использование информации;

– $R^2(M)$ – компонента вероятности, рассчитанная на основании вероятностей обнаружения сигнала;

– $R^3(M)$ – компонента вероятности, рассчитанная на основании анализа предрасположенности противника к реализации конкретного типа атаки;

– $L(M)$ – оценка финансовых потерь владельца информации от РУ способом М;

– $L(M) = L(Md) + L(Mr)$, где:

– $L(Md)$ – оценка финансовых потерь за счет нарушения средств защиты объекта РЭС в процессе проведения атаки.

– $L(Mr)$ – оценка финансовых потерь за счет использования информации противником.

Для расчета оценок финансовых потерь используются следующие статистические данные:

– $L(e(Mu))$ – ущерб владельца от нарушения функционирования РЭС в процессе успешного перехвата сигнала в инциденте $e(M)$;

– $L(e(Mr))$ – ущерб владельца от успешного использования информации в инциденте $e(M)$ (утечка технологий, утрата стратегического преимущества, судебные издержки и т.д.).

Для расчета оценок финансовых потерь организации от реализации угроз используются следующие экспертные оценки:

– $Le(o,u(o))$ – экспертная оценка потерь от действия а на объект o;

– $Le(d,u(d))$ – экспертная оценка финансовых потерь за счет использования противником раскрытых сведений.

4.2. Расчет риска при успешном проведении атаки на объект РЭС

Для расчета риска при успешном проведении атаки на объект РЭС введем следующие обозначения:

$RISK$ – величина риска для объекта РЭС;

$RISK_{full}(M)$ – оценка риска реализации угрозы способом M;

$RISK_{full}(M) = L(M) \cdot R(M)$;

$RISK_{full}(d)$ – оценка риска для охраняемых сведений d. Определяется как максимальный риск реализации угрозы для данных сведений.

Создание СЗИ РЭС с заданными стоимостными параметрами и уровнем снижения риска предполагает затраты C. Учитывая возможность появления различных случайных факторов, затраты на создание СЗИ РЭС можно представить как $C = F(C';S;y)$ – общая стоимость СЗИ (совокупная стоимость владения), где:

– S – состав СЗИ РЭС;

– $C' = \sum_{i=1}^{m} \frac{(K_i + n_i \cdot C_i^m) + y_i}{b_i} = \sum_{i=1}^{m} \frac{c_i + y}{b_i}$, где c_i – стоимость реализации i -ой меры защиты, которая складывается из:

– $c_i = c_{i_{\text{стоимость средства защиты}}} + c_{i_{\text{прочие расходы}}} = K_i + n_i \cdot C_i^m$;

– y – суммарный остаточный ущерб после применения мер защиты;

Пусть $a'_{i,j}$, $a''_{i,j}$ прогнозируемый и остаточный ущербы до и после применения i -й меры защиты для j-й угрозы, b_i – разница между прогнозируемым ущербом до применения i-й контрмеры и остаточным ущербом, y_i-суммарный остаточный ущерб после применения i-й контрмеры.

Матрица прогнозируемого ущерба:

Меры защиты \ Угрозы	u_1	...	u_n
k_1	a'_{11}	...	a'_{1n}
⋮	⋮	⋱	⋮
k_m	a'_{m1}	...	a'_{mn}

Матрица остаточного ущерба:

Меры защиты \ Угрозы	Mu_1	...	Mu_n
k_1	a''_{11}	...	a''_{1n}
⋮	⋮	⋱	⋮
k_m	a''_{m1}	...	a''_{mn}

$y_i = \sum_{j=1}^{n} a''_{ij}$, где $i = \overline{1,m}$.

$b_i = \sum_{j=1}^{n} (a'_{ij} - a''_{ij})$, где $i = \overline{1,m}$.

$y = \sum_{i=1}^{m} \left(\frac{c_i + y_i}{b_i}\right) k_i$.

– K_i – капитальные (закупка, создание) затраты на -ю меру защиты;

– C_i^m – эксплуатационные затраты на -ю меру защиты;

– n_i – количество планируемых лет эксплуатации меры защиты (прогнозируется по результатам анализа развития технических возможностей нарушителя);

$$K_i = K_b + K_m + K_d + K_e + K_t,$$

где:

– K_b – затраты на проектирование меры защиты;

– K_m – затраты на технические средства;

– K_d – затраты на внедрение меры защиты;

– K_e – затраты на обучение персонала;

– K_t – затраты на тестирование меры защиты;

$$C_i^m = C_{ic}^m + C_{ia}^m + C_{ie}^m + C_{io}^m,$$

где:

– C_{ic}^m – зарплата сотрудников, эксплуатирующих меру защиты (служба безопасности);

– C_{ia}^m – амортизационные отчисления;

– C_{ie}^m – затраты на техническое обслуживание;

– C_{io}^m – прочие затраты;

$I(k)$ – экспертная оценка косвенной выгоды от внедрения меры защиты (сокращение штата, количества необходимых контрольных мероприятий и т.д.);

$Rent$ – оценка экономической обоснованности СЗИ.

4.3. Алгоритм анализа рисков и оценки экономической эффективности

Алгоритм анализа рисков и оценки экономической эффективности состоит из следующих этапов:

1. Определение потенциальных противников i, $i \in \{i_1, \dots, i_{n_i}\}$ ведущих перехват сигналов, излучаемых РЭС;

2. Описание объекта защиты:

2.1. описание объектов, на которые может проводиться атака o, $o \in \{o_1, \dots, o_{n_o}\}$;

2.2. описание охраняемых сведений d, $d \in \{d_1, \dots, d_{n_d}\}$;

2.3. описание действий, предпринимаемых противником при взаимодействии с объектом атаки $u(o)$, $u(o) \in \{u_1, \dots, u_{n_{uo}}\}$ и с перехваченной информацией $u(d)$, $u(d) \in \{u_1, \dots, u_{n_{ud}}\}$;

3. Выбор мер защиты на основе данных анализа нарушителей и объекта защиты:

3.1. формирование набора мер защиты, применимых для защиты объекта и охраняемых сведений $k(o_1, \dots, o_{n_o})$, $k(d_1, \dots, d_{n_d})$.

3.2. формирование матрицы угроз:

Меры защиты	Угрозы: Mu_1	…	Mu_n
k_1	a_{11}	…	a_{1n}
⋮	⋮	⋱	⋮
k_m	a_{m1}	…	a_{mn}

где $a_{i,j}$ – коэффициенты покрытия.

4. Получение экспертных оценок:

4.1. $K_i(k), C_i^m(k)$ – затраты на -ю меру защиты $k \in \{k_1, \dots, k_{n_k}\}$;

4.2. $I(k)$ – косвенная выгода от внедрения меры защиты k, $k \in \{k_1, \dots, k_{n_k}\}$;

4.3. $Le(o, u(o))$ – экспертная оценка потерь от действия u на объект o, $o \in \{o_1, \dots, o_{n_o}\}$, $u(o) \in \{u_1, \dots, u_{n_{uo}}\}$;

4.4. $Le(d, u(d))$ – экспертная оценка финансовых потерь за счет использования противником раскрытых сведений d, $d \in \{d_1, \dots, d_{n_d}\}$, $u(d) \in \{d_1, \dots, d_{n_{ud}}\}$.

5. Описание типа атаки:

5.1. Выявление способов перехвата информации. Как правило, перехват осуществляется путем сканирования сигналов, излучаемых объектом атаки и выделения из них охраняемых сведений определенным способом:

$Mu(d,i) \in \{Mu_1, \dots, Mu_{n_{Mu}}\}$;

$Mu(d,i) = \{(o, u(o)) | o \in \{o_1, \dots, o_{n_o}\},$

$a(o) \in \{u_1, \dots, u_{n_{uo}}\}\}$.

5.2. Выявление способов использования противником перехваченных данных:

$Mr(d,i) \in \{Mr_1, \dots, Mr_{nMr}\}$;

$Mr(d,i) = \{(d, u(d)) | d \in \{d_1, \dots, d_{n_d}\},$

$u(d) \in \{u_1, \dots, u_{n_{ud}}\}\}$.

5.3. Определение способов реализации угроз как комбинации способов перехвата сигнала и способов использования перехваченных данных:

$M(d,i) \in \{M_1, \dots, M_{n_m}\}$;

$M(d,i) = \{(Mu(d,i); Mr(d,i)) |$

$|Mu(d,i) \in \{Mu_1, \dots, Mu_{n_{Mu}}\},$

$Mr(d,i) \in \{Mr_1, \dots, Mr_{n_{Mr}}\}\}$.

5.4. Оценка параметров, характеризующих способы перехвата информации $M(d,i) \in \{M_1, \dots, M_{n_m}\}$: $G(M), O(d,i)$, где $O(d,i) = 0$ по умолчанию.

6. Фиксация значений:

6.1. Определение конкретной информации (охраняемые сведения) d, $d \in \{d_1, \dots, d_{nd}\}$.

6.2. Фиксация конкретного нарушителя $i, i \in \{i_1, \dots, i_{n_i}\}$.

6.3. Фиксация конкретного способа реализации угрозы:

$$M(d,i) = (Mu(d,i); Mr(d,i))\ M\{M_1, \dots, M_{n_m}\}.$$

7. Анализ статистических данных об атаках:

7.1. Описание атак:

$$e(M), e(M) \in \{e_1, \dots, e_{n_e}\},\ e(M) = (e(Mu); e(Mr)).$$

7.2. Указание ущерба владельца от реализаций атак: $L(e(Mu)), L(e(Mr))$.

7.3. Указание успешных и предотвращенных атак $Nf(Mu), Nf(Mr), Ns(Mu), Ns(Mr)$:

$Ns(Mu) + Nf(Mu) = N_u > 0$, где N_u – коэффициент успеха;

$Ns(Mr) + Nf(Mr) = N_r > 0$, где N_r – коэффициент предотвращения.

По умолчанию $N_u = N_r = 1$.

7.4. Расчет оценки вероятности реализации угрозы на основании статистики атак (в случае отсутствия данных не рассчитывается):

$$R^1(M) = R^1(Mu) \cdot R^1(Mr),\ 0 \le R^1(M) \le 1,$$

$$R^1(Mu) = \frac{Ns(Mu)}{Ns(Mu)+Nf(Mu)},\ R^1(Mr) = \frac{Ns(Mr)}{Ns(Mr)+Nf(Mr)}.$$

8. Расчет оценки компоненты вероятности реализации угрозы на основании вероятностей обнаружения сигнала:

8.1. Расчет вероятности обнаружения сигнала объекта и вспомогательных средств.

Данный расчет целесообразно проводить для всех рассматриваемых угроз.

В результате формируется матрица вероятностей:

Угрозы

Меры защиты	Mu_1	...	Mu_n
k_1	p_{11}	...	p_{1n}
⋮	⋮	⋱	⋮
k_m	p_{m1}	...	p_{mn}

$$p'_i = \prod_{j=1}^{m} p_{ij} \to min_k, \text{ где } i = \overline{1,n};$$

p'_i – вероятность обнаружения сигнала после применения выбранных мер защиты.

Вероятность обнаружения сигнала вспомогательных средств рассчитывается аналогично:

$$R^2(M) = R_o,\ 0 \le R^2(M) \le 1.$$

8.2. Расчет вероятности реализации угрозы на основании предрасположенности противника к реализации конкретного типа атаки:

$$R^3(M) = \frac{G(M) - V(M) - O(d,i)}{G(M)},\ 0 \le R^3(M) \le 1.$$

9. Вычисление общей оценки вероятности реализации угрозы:

$$R(M) = \frac{\sum_\mu k_\mu \cdot R^\mu(M)}{\sum_\mu k_\mu}, \mu = 1, \dots, 3,\ 0 \le R(M) \le 1.$$

Коэффициенты: k_1 – статистический, k_2 – технический, k_3 – мотивационный.

Коэффициенты рассчитываются следующим образом:

Пусть N – граничное значение, задаваемое экспертом, по умолчанию N=10.

$k_\mu = 0$, если R^μ не оценено, $\mu = \overline{1,3}$;

$k_1 = \log(N_u + N_r)$ при $N_a + N_r \le N$;

$k_1 = 1$ при $N_u + N_r > N$;

$k_\mu = 1$, если R^μ рассчитано, $\mu = 2,3$.

10. Расчет оценок риска для способа реализации угроз:

10.1. Расчет оценки ущерба от атаки:

$$L(M) = L(Mu) + L(Mr),$$

где $L(Mu)$ – ущерб от перехвата охраняемых сведений, рассчитывается на основании статистики инцидентов и на основании суммарных потерь от действий u на объекты защиты o:

$$L(Ma) = \frac{\frac{k_1}{Ns(Mu)} \cdot \sum_o L(e(Mr)) + Le(o, u(o))}{k_1 + 1},\ o \in Mu;$$

$$L(Mr) = \frac{\frac{k_1}{Ns(Mr)} \cdot \sum_o L(e(Mr)) + Le(d, u(d))}{k_1 + 1},$$ где k_1 – статистический коэффициент.

10.2. Расчет оценки риска для способа атаки:

$$RISK_{full}(M) = L(M) \cdot R(M).$$

10.3. Расчет оценки возможности, что атака не будет реализована:

$$\overline{RISK_{full}(M)} = L(M) \cdot (1 - R(M)).$$

11. Выбор следующих, не рассмотренных, значений:

11.1. Рассмотрение всех существующих угроз $M(d,i)$. Переход к п. 6.3 и выбор следующей угрозы. В случае рассмотрения всех значений переход к п. 11.2.

11.2. Рассмотрение всех потенциальных противников i_n. Переход к п. 6.2 и выбор следующего

противника. В случае рассмотрения всех значений переход к п. 12.

12. Нахождение риска для охраняемых сведений.

Риск для охраняемых сведений – максимальный риск по всем способам реализации угроз для данных сведений:

$$RISK_{full}(d) = \max_M RISK_{full}(M(d,i)) =$$

$$= RISK_{full}(M^{max}(d)),$$ соответствует способу реализации угрозы $M^{max}(d), M \in \{M_1, \dots, M_{nm}\}$.

$\overline{RISK_{full}(M)}$ – величина ущерба, который мог быть нанесен при реализации угрозы с максимальным риском для охраняемых сведений:

$$\overline{RISK_{full}(d)} = \overline{RISK_{full}(M^{max}(d))}.$$

13. Проведение расчетов для всех охраняемых сведений d. Переход к п. 6.1 и выбор не рассмотренных сведений. В случае рассмотрения всех значений переход к п. 14.

14. Нахождение максимального и минимального риска для СЗИ объекта:

$RISK^{max}=\max_d RISK(d)$, что соответствует способу реализации угрозы M^{max};

$RISK^{min}=\min_d RISK(d)$, что соответствует способу реализации угрозы M^{min};

$i \in \{d_1, \dots, d_{nd}\}$.

15. Вычисление оценки рентабельности СЗИ РЭС:

$$Rent = \frac{\sum_d \overline{RISK_{full}(d)} + \sum_k I(k) - C}{C},$$ где $C = F(C'; S; y)$.

Использование экспертной оценки косвенной выгоды $I(k)$ позволяет обеспечить гибкий подход, охватывающий не только конкретные затраты на меры и средства защиты информации и их обеспечение, но и вторичные факторы (сокращение штата, количества необходимых контрольных мероприятий и т.д.), часто имеющие существенное влияние на экономическую обоснованность создаваемой СЗИ РЭС.

16. Анализ результатов.

В зависимости от рассчитанного значения $Rent$ можно сделать выводы об экономической обоснованности проектируемой СЗИ РЭС.

Если получено, что $Rent \leq 0$, затраты на СЗИ РЭС превышают выгоду от ее функционирования. В данном случае будет целесообразно пересмотреть выбор мер защиты, остановившись на менее затратных решениях. Так же можно принять некоторые риски или передать их на аутсорсинг. После корректировки необходимо провести повторный расчет.

Если получено, что $Rent > 0$, то существует возможность использовать дополнительные меры защиты для снижения максимальных рисков. После корректировки необходимо провести повторный расчет.

Выводы

В данной статье предложена процедура анализа рисков и оценки экономической обоснованности, создаваемой СЗИ РЭС.

Предложенная процедура позволяет:

- осуществлять создание СЗИ на основе анализа реальной информации об объекте защиты, потенциальных нарушителях, рисках и угрозах, что повышает гибкость системы при появлении новых угроз и нарушителей;
- дать объективную оценку угрозам и оценить экономическую обоснованность создаваемой СЗИ РЭС не только на основе затрат на построение системы, но исходя из данных о потенциальном снижении ущерба от утечки конфиденциальной информации и вероятности распознавания сигнала РЭС, благодаря качественному подходу, применяемому при анализе рисков;
- учесть всю специфику исследуемой области путем использования модели возникновения нарушения установленных требований (норм) эффективности защиты информации на объекте (угроз);

модернизировать СЗИ РЭС на основе данных полученных в результате проведения контрольных мероприятий.

Предлагаемая процедура, в первую очередь, ориентирована на организации, проводящие разработку и проектирование РЭС и заинтересованные в нахождении баланса между затратами на построение СЗИ и достигаемым уровнем безопасности (снижением вероятности обнаружения сигналов РЭС). Однако стоит отметить, что, не смотря на имеющуюся ориентированность процедуры на заданную область, ее части могут быть использованы любыми организациями для проведения экономического обоснования создаваемых СЗИ и организации защиты информации в целом.

Литература:

1. ГОСТ РВ 15.203 – 2001 СРПП ВТ. Порядок выполнения опытно-конструкторских работ по созданию изделий и их составных частей. Основные положе-ния. М., 2003. 117 с.
2. Мельников Ю.П. Воздушная радиотехническая разведка. М.: Изд-во Радиотех-ника, 2005. 304 с.
3. Вакин С.А., Шустов Л.Н. Основы радиопротиводействия и радиотехнической разведки. М.: Изд-во Советсткое радио, 1968. 448 с.
4. Палий А.И. Радиоэлектронная борьба. М.: Изд-во Воениздат, 1981. 272 с.
5. Вартанесян Е.А. Радиоэлектронная разведка. М.: Изд-во Воениздат, 1991. 255 с.
6. Хорев А.А. Технические средства и способы промышленного шпионажа. М.: ЗАО «Дальснаб», 1997.
7. Абалмазов Э.И. Методы и инженерно-технические средства противодействия информационным угрозам. – М.: Гротэк, 1997.
8. Лунегов А.Н., Рыжов А.Л. Технические средства и способы добывания и защиты информации. – М.: ВНИИ «Стандарт», 1993.
9. Троицкий И.И., Репин М.М. Организация работы по защите информации на эта-пе испытаний опытного образца радиоэлектронной техники // «Безопасные информационные технологии». Сборник трудов Второй всероссийской научно-технической конференции/ под ред. Матвеева В.А. – М: Изд-во НИИ радиоэлектроники и лазерной техники, 2011 г. С 136-138.

References:

1. GOST RV 15.203 – 2001 SRPP VT Poryadok vypolneniya opytno - konstruktorskikh rabot po sozdaniyu izdeliy i ikh sostavnykh chastey . Osnovnyye polozheniya. M., 2003. 117 c.
2. Mel'nikov Y.P. Vozdushnaya radiotekhnicheskaya razvedka. M.: Izd-vo Radiotekhnika, 2005. 304 s
3. Vakin S.A., Shustov L.N. Osnovy radioprotivodeystviya i radiotekhnicheskoy razvedki. M.: Izd-vo Sovetstkoye radio, 1968. 448 s.
4. Paliy A.I. Radioelektronnaya bor'ba. M.: Izd-vo Voyenizdat, 1981. 272 s.
5. Vartanesyan Y.A. Radioelektronnaya razvedka. M.: Izd-vo Voyenizdat, 1991. 255 s.
6. Khorev A.A. Tekhnicheskiye sredstva i sposoby promyshlennogo shpionazha. M.: ZAO «Dal'snab», 1997.
7. Abalmazov E.I. Metody i inzhenerno-tekhnicheskiye sredstva protivodeystviya informatsionnym ugrozam. M.: Grotek, 1997.
8. Lunegov A.N., Ryzhov A.L. Tekhnicheskiye sredstva i sposoby dobyvaniya i zashchi-ty informatsii. M.: VNII «Standart», 1993.
9. Troitskiy I.I., Repin M.M. Organizatsiya raboty po zashchite informatsii na etape ispytaniy opytnogo obraztsa radioelektronnoy tekhniki // «Bezopasnyye informa-tsionnyye tekhnologii». Sbornik trudov Vtoroy vserossiyskoy nauchno-tekhnicheskoy konferentsii / pod red. Matveyeva V.A. M: Izd-vo NII radioelektroniki i lazernoy tekhni ki-2011 g. S136-138.