## *КРАТКИЕ СООБЩЕНИЯ*

*УДК 621.391.25*

# МЕТОД ОЦЕНКИ ЭФФЕКТИВНОСТИ ИЕРАРХИЧЕСКОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ И ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В.В. МАЛИКОВ, Т.В. БОРБОТЬКО

*Белорусский государственный университет информатики и радиоэлектроники*
*П. Бровки, 6, Минск, 220013, Беларусь*

*Поступила в редакцию 25 ноября 2009*

Предложен метод оценки эффективности иерархической системы информационной и инженерно-технической защиты объектов от несанкционированного доступа с учетом их этапов жизненного цикла.

*Ключевые слова:* иерархическая система информационной и инженерно-технической защиты объектов, метод оценки эффективности, этапы жизненного цикла.

Одной из важных задач при проектировании и анализе функционирования современных систем информационной и инженерно-технической безопасности для объектов различных категорий является оценка эффективности системы защиты объекта, устанавливающей уровень ее соответствия определенным критериям [1].

Существующие в настоящее время методы оценки эффективности системы защиты объекта, а также программные комплексы, разработанные на их основе, имеют определенный перечень недостатков и уязвимостей, а также значительную (во многих случаях избыточную) стоимость и низкую функциональность.

Целью настоящей работы является разработка метода оценки эффективности иерархической системы информационной и инженерно-технической защиты объектов с учетом этапов ее жизненного цикла. В качестве действенного способа решения такой задачи предлагается использование метода оценки эффективности на основе профилей безопасности [2].

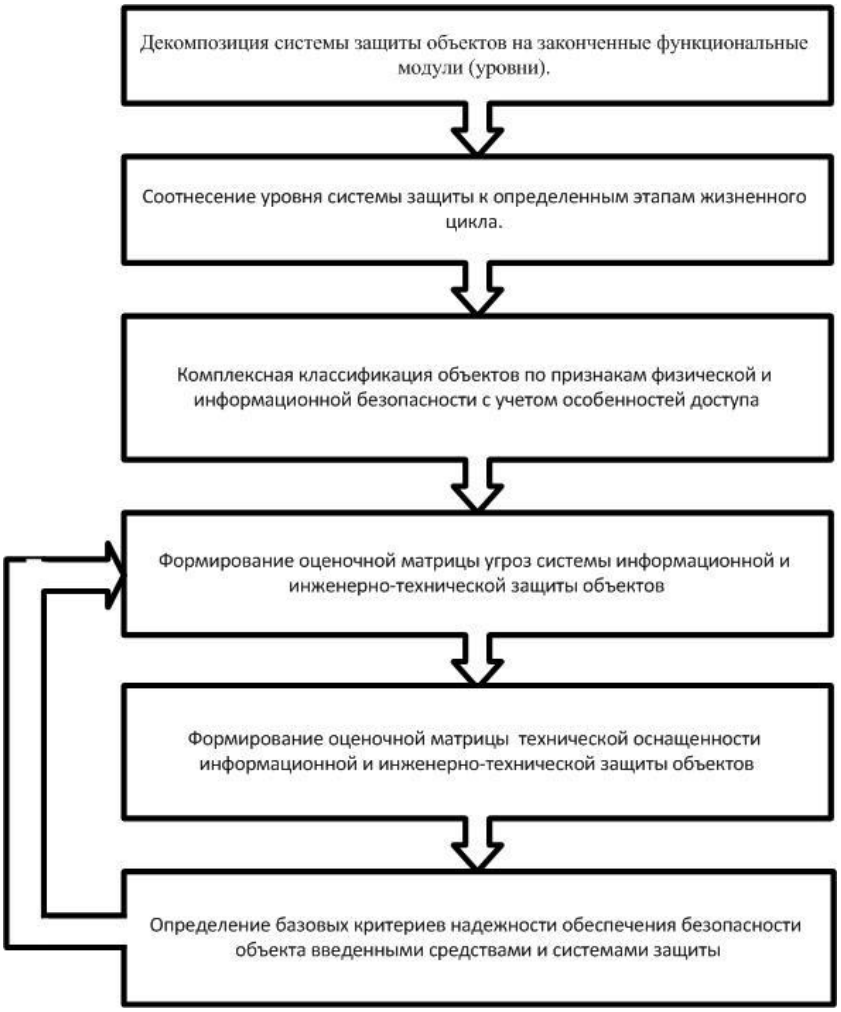
Оценку информационной и инженерно-технической защиты объектов различных категорий возможно проводить в следующем порядке (показано на рисунке):

1. Декомпозиция системы защиты объектов на законченные функциональные модули (уровни). Предлагается использование варианта декомпозиции, который учитывает полный цикл обеспечения защиты, начиная с этапа детектирования угрозы до реагирования на инцидент в сфере безопасности: объектовый уровень, уровень каналов сопряжения и телекоммуникации, уровень обеспечения и управления безопасностью [3].

К объектовому уровню относятся технические средства и системы обеспечения физической безопасности (охранно-пожарная сигнализация, системы пожаротушения и оповещения о пожаре, автоматическая система контроля и управления доступом (АСКУД), система видеонаблюдения (СВН), средства инженерно-технической укрепленности), аппаратно-программный комплекс мониторинга состояния систем жизнеобеспечения объекта

(энергоснабжение, системы вентиляции и кондиционирования, водоснабжение и канализация, мониторинг концентрации токсичных веществ, радиационный контроль), программно-технические средства и системы обеспечения информационной безопасности (средства криптографической защиты информации, средства защиты информации от несанкционированного доступа, средства подавления и др.).

Уровень каналов сопряжения и телекоммуникации предназначен для передачи служебных информационных сигналов о состоянии объекта охраны в единый информационно-аналитический центр по сбору, отработке, принятию решений по безопасности охраняемых объектов, который относится к уровню обеспечения и управления безопасностью.




Метод оценки эффективности иерархической системы информационной и инженерно-технической защиты объектов от несанкционированного доступа

2. Следующим этапом является соотнесение уровня системы защиты к определенным этапам жизненного цикла [4]. В настоящей методике будем принимать во внимание следующие этапы жизненного цикла системы защиты объектов:

– проектирование и построение;
– внедрение;
– эксплуатация;
– модернизация / утилизация.

3. Проведение комплексной классификации объектов по признакам физической и информационной безопасности с учетом особенностей доступа с отнесением к следующим группам объектов:

– с упрощенным доступом;
– с ограниченным доступом;
– с важным доступом;

– доступ с расширенной защитой;

– доступ с максимальной защитой.

Для осуществления комплексной классификации объектов по признакам физической и информационной безопасности с учетом особенностей доступа введем следующие категории безопасности: организационная структура управления объектом, функционально-экономическое построение процесса организации деятельности объекта, оценка риска.

4. Далее формируется оценочная матрица угроз иерархической системы информационной и инженерно-технической защиты объектов.

4.1. Проводится классификация угроз иерархической системы информационной и инженерно-технической защиты объектов с учетом этапов жизненного цикла.

Отнесение угрозы к той или иной категории выполняется методом экспертных оценок. Для классификации угроз безопасности используются следующие их категории в соответствии с этапами жизненного цикла системы:

а) проектирование и построение:

– угрозы, возникающие при проектировании системы защиты;

– угрозы, возникающие при классификации и категорировании объекта защиты;

б) внедрение:

– угрозы, связанные с реализацией структуры внедрения;

– угрозы, связанные с процессами квалификации, обучения и контроля качества выполняемых работ;

в) эксплуатация:

– угрозы, связанные с нарушением безопасности системы;

– реагирование на угрозы безопасности: с введением специальных планов и без введения специальных планов;

г) модернизация / утилизация:

– угрозы, связанные с перспективной модернизацией / утилизацией;

– угрозы, связанные с текущей модернизацией / утилизацией.

Для того чтобы исключить ошибочное отнесение угрозы к той или иной категории предлагается проводить анализ угрозы по следующим критериям: характер ее воздействия, цель воздействия, условия начала воздействия, механизм реализации [5].

4.2. На основе метода экспертных оценок с учетом статистических данных по вопросам информационной и физической безопасности, а также имущественных преступлений проводится выставление вероятности реализации классифицированных угроз $p_i$=0÷1 и значимости их реализации — $v_i$.

При проведении указанной выше оценки принимаем следующие положения:

– угрозы системы безопасности являются независимыми событиями, т.е. появление угрозы $A$ не влияет на вероятность угрозы $B$, т.е. $P_A(B)=P(B)$;

– суммарная значимость реализации вида угроз $v$=1, т.е. оценки значимости по виду угроз, образует полную группу событий (реализация хотя бы одной из угроз является достоверным событием).

4.3. Величина угрозы на уровень системы безопасности представляет собой произведение вероятности реализации угрозы на величину значимости угрозы.

4.4. Уровень по виду угроз для этапа жизненного цикла уровня безопасности системы вычисляется как вероятность появления хотя бы одного из $n$-независимых событий.

4.5. Уровень по видам угроз по этапу жизненного цикла уровня безопасности системы определяется как вероятность появления хотя бы одного из $m$-независимых событий.

4.6. Уровень угроз по всем этапам жизненного цикла уровня безопасности вычисляется как вероятность $k$-независимых событий.

4.7. Общий риск потерь по уровню системы безопасности равен произведению общего уровня угроз на величину критичности ресурса (денежное выражение), которая определяется системой критериев:

– ущерб репутации организации;

– безопасность персонала;

– разглашение коммерческих сведений;

– финансовые потери и др.

5. Далее формируется оценочная матрица технической оснащенности информационной и инженерно-технической защиты объектов.

5.1. Проводится классификация технической оснащенности системы информационной и инженерно-технической защиты объектов.

В качестве типовых программно-технических средств для построения систем защиты предлагается использование следующих компонентов:

– технологии передачи данных;

– операционные системы (ОС);

– системы управления базами данных (СУБД);

– аппаратно-программные средства защиты информации.

В качестве типовых физических средств для построения систем защиты предлагается использование основных и вспомогательных технических, инженерно-технических средств и систем охраны.

К основным средствам и системам охраны будем относить:

а) технические средства и системы охраны периметра;

б) технические средства и системы охраны зданий и помещений:

– охранная сигнализация.

– технические средства противопожарной защиты и оповещения (устройства пожарной автоматики: системы пожарной сигнализации, системы пожаротушения в автоматическом режиме; системы оповещения о пожаре);

в) средства инженерно-технической укрепленности периметра, зданий и помещений.

К вспомогательным средствам и системам охраны будем относить:

а) СВН;

б) АСКУД и др.

5.2. На основе метода экспертных оценок с учетом технической оснащенности системы информационной и инженерно-технической защиты объектов проводится выставление значимости средств защиты, образующих логически законченную подсистему защиты.

При проведении оценки значимости принимаем следующие положения:

– логические законченные подсистемы защиты являются независимыми модулями, т.е. вероятность отражения угрозы подсистемой $A$ не влияет на вероятность отражения угрозы подсистемой $B$, т.е. $P_A(B)=P(B)$;

– суммарная оценочная значимость средств защиты, образующих логически законченную подсистему защиты $w=1$, т.е. оценки значимости по подсистеме защиты образуют полную группу событий (отражение идентифицированной угрозы одним из средств защиты является достоверным событием).

6. Затем определяем базовые критерии надежности обеспечения безопасности объекта введенными средствами и системами защиты.

6.1. Технический критерий эффективности средств и систем защиты — $K_{ЭФ/Т}$:

– позволяет определить техническую эффективность введенных средств и систем защиты, т.е. вероятность отражения атак (0÷1);

– определяется на основе оценочной матрицы технической оснащенности информационной и инженерно-технической защиты объектов;

– будем считать, что вероятность успешного отражения атаки принимается при $K_{ЭФ/Т}=0,9\div1,0$;

– обеспечение $K_{ЭФ/Т}=0,9\div1,0$ является условием проведения дальнейшего анализа по экономическому критерию эффективности;

– общий технический критерий эффективности по трем уровням безопасности определяется как вероятность $h$-независимых событий.

6.2. Экономический критерий эффективности средств и систем защиты — $K_{ЭФ/Т}=0,9\div1,0$:

– позволяет определить экономическую эффективность введенных средств и систем защиты, т.е. соотношение стоимости введенных технических средств и систем защиты $S_{защ}$ к суммарной стоимости потерь по ресурсам объекта $P$, которая определяется критериями: ущерб репутации организации, безопасность персонала, разглашение коммерческих сведений, финансовые потери и др.;

– определяется на основе оценочной матрицы угроз иерархической системы информационной и инженерно-технической защиты объектов;

– будем считать, что рекомендуемое значение успешного экономического применения средств и систем защиты должно быть $K_{ЭФ/Э} \geq 1$.

Разработан метод оценки эффективности информационной и инженерно-технической защиты объектов различных категорий на основе профилей безопасности, который позволяет проводить анализ и динамическую коррекцию результатов оценки с учетом [6]:

– появления новых, ранее не классифицированных видов угроз, а также изменения приоритетов оценки, углубления и детализации ранее классифицированных угроз;

– разработки новых средств и систем безопасности в области информационной и инженерно-технической защиты объектов различных категорий, а также изменения приоритетов в оценке действующих систем защиты на основе анализа их эффективности.

Использование технического и экономического критериев оценки системы защиты позволяет получить численные значения оценки эффективности (вероятность отражения угроз не менее 90%) с учетом затрат на обеспечение защиты объектов (вариация от 8 до 25% от общей стоимости ресурсов) [7].

## METHOD OF AN ESTIMATION OF EFFECTIVENESS OF HIERARCHICAL SYSTEM OF INFORMATIONAL AND TECHNICAL PROTECTION OF OBJECTS FROM UNAUTHORIZED ACCESS

V.V. MALIKOV, T.V. BORBOTKO

**Abstract**

The method of an estimation of effectiveness of hierarchical system of informational and technical protection of objects with allowance for their stages of life cycle is offered.

**Литература**

1. *Маликов В.В.* // Технологии безопасности. 2009. № 1. С. 46–47.
2. *Маликов В.В.* // Докл. БГУИР. 2009. № 2. С. 99–104.
3. *Маликов В.В., Борботько Т.В.* // Вес. Воен. акад. Респ. Беларусь. 2007. № 4. С. 128–132.
4. ISO/IEC 15288:2008 // ISO [Электрон. ресурс]. — 2008. — Режим доступа: http://www.iso.org/iso/catalogue_detail?csnumber=43564. — Дата доступа: 10.06.2009.
5. *Лыньков Л.М., Маликов В.В., Борботько Т.В.* Защита объектов различных форм собственности от несанкционированного доступа: монография / Под ред. Л.М. Лынькова. Минск, 2008.
6. *Маликов В.В.* // Материалы докладов и краткие сообщения 7-й Белорусско–российской НТК "Технические средства защиты информации". Минск, 23–24 июня 2009 г. Минск, 2009. С. 8.
7. *Маликов В.В.* // Сетевые решения. 2008. № 4. С. 68–80.