

**Оценка защищенности объектов информатизации
на основе математического моделирования как альтернатива
сертификационным испытаниям**

Сычев А.М.³⁴⁸, Сухорукова Н.А.³⁴⁹, Холод Д.А.³⁵⁰

В данной статье показана возможность получения численной оценки защищенности объектов информатизации с использованием математического моделирования угроз информационной безопасности, вызванных противоправными действиями, и процессов реагирования на такого рода действия. Данный подход позволит оценивать эффективность различных мер реагирования и на основе этих оценок обосновывать наиболее эффективную систему обеспечения защищенности объектов информатизации.

Ключевые слова: объекты информатизации, математическое моделирование, информационная безопасность, оценка защищенности, сертификационные испытания.

Введение

Постоянное совершенствование методов несанкционированного доступа (НСД) к информации, а также значительный ущерб, наносимый такого рода действиями, обусловили целенаправленное и системное совершенствование технологий обеспечения информационной безопасности и механизмов реагирования на угрозы безопасности информации [1-3]. При этом одним из основных направлений совершенствования является обеспечение соответствия характеристик этих механизмов требованиям адекватного реагирования на угрозы и, как следствие, адекватной оценки эффективности мер реагирования.

Очевидно, что подобная оценка должна осуществляться системно [4], на основе всестороннего исследования способов обеспечения безопасности объектов информатизации (ОИ).

В соответствии с системным подходом исследование механизмов реагирования на угрозы безопасности информации ОИ связано с оценкой защищенности ОИ, т.е. возможностей этих механизмов адекватно реагировать на угрозы информационной безопасности ОИ.

Существующая концепция оценки защищенности ОИ на основе сертификационных испытаний

Базовой концепцией, реализуемой в практике оценки защищенности ОИ, является концепция сертификационных испытаний. В рамках данной концепции предполагается оценка защищенности ОИ путем сертификации используемых средств защиты информации от несанкционированного доступа (НСД). В соответствии с Руководящим документом (РД) ФСТЭК «Защита от несанкционированного доступа к информации. Термины и определения» под сертификацией средств защиты информации понимается деятельность по подтверждению соответствия возможностей средств защиты информации требованиям государственных стандартов, нормативных документов, утверждаемых Правительством Российской Федерации и федеральными органами по сертификации в пределах компетенции этих органов. Следует отметить, что, в соответствии с данным РД сертификационные исследования ограничиваются описанием состава функций, выполняемых механизмами защиты информации от НСД, и качественной характеристикой

³⁴⁸ Сычев Артем Михайлович, к.т.н., доцент, МГТУ им. Н.Э. Баумана, Москва, zi@bmstu.ru

³⁴⁹ Сухорукова Надежда Алексеевна, МГТУ им. Н.Э. Баумана, Москва, zi@bmstu.ru

³⁵⁰ Холод Денис Александрович, МГТУ им. Н.Э. Баумана, Москва, zi@bmstu.ru

содержания этих функций, соответствующих определенным классам защищенности информационных систем и средств вычислительной техники (СВТ), а также перечнем нормативных документов по указанной проблеме. Реализуемые при этом методики сертификации состоят в проверке заявленных возможностей предъявляемым требованиям (табл.1). В соответствии с РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» вывод о неэффективности механизма защиты информации в целом делается в случае, если хотя бы одна из заявленных возможностей отсутствует.

Таблица 1.

Соответствие заявленных возможностей по защите информации классам защищенности объектов информатизации

Используемые средства защиты информации и требования к ним	Классы защищенности				
	1Д	1Г	1В	1Б	1А
1. Средства управления доступом					
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:					
к ОИ	+	+	+	+	+
к терминалам, средствам вычислительной техники (СВТ), узлам компьютерной сети, каналам связи, внешним устройствам СВТ	-	+	+	+	+
к программам	-	+	+	+	+
к данным	-	+	+	+	+
1.2. Управление потоками информации					
2. Средства регистрации и учета					
2.1. Регистрация и учет:					
входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+	+	+	+
выдачи печатных (графических) выходных документов	-	+	+	+	+
запуска (завершения) программ и процессов (заданий, задач)	-	+	+	+	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	+	+	+	+
доступа программ субъектов доступа к терминалам, СВТ, узлам компьютерной сети, каналам связи, внешним устройствам СВТ, программам и данным	-	+	+	+	+
изменения полномочий субъектов доступа	-	-	+	+	+
создаваемых защищаемых объектов доступа	-	-	+	+	+
2.2. Учет носителей информации					
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти СВТ и внешних накопителей					
2.4. Сигнализация попыток нарушения защиты					
3. Криптографические средства					
3.1. Шифрование конфиденциальной информации					
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах					
3.3. Использование аттестованных (сертифицированных) криптографических средств					

4. Средства обеспечения целостности рабочей среды СВТ					
4.1. Обеспечение целостности программных средств и обрабатываемой информации	-	-	-	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в информационной системе	+	+	+	+	+
4.4. Периодическое тестирование рабочей среды СВТ	-	-	+	+	+
4.5. Наличие средств восстановления информации	+	+	+	+	+
4.6. Использование сертифицированных средств защиты	-	-	+	+	+

Очевидным достоинством данной концепции оценки защищенности ОИ является простота процедур оценки. Недостатками, ограничивающими ее использование, являются:

1) отсутствие формальной интерпретации характеристик угроз безопасности информации;

2) отсутствие формализованного представления динамики воздействия угроз безопасности информации и процессов реагирования на такого рода угрозы;

3) отсутствие формализованной модели нарушения безопасности информации, учитывающей особенности действий нарушителя как источника угроз.

Указанные недостатки приводят к множеству ошибок при обосновании способов и средств защиты информации [5], что, в свою очередь, обуславливает необходимость поиска таких подходов к оценке защищенности ОИ, которые бы обеспечивали требуемую адекватность оценки.

Предлагаемая концепция оценки защищенности ОИ на основе математического моделирования

Как показывает практика проведения исследований в этом направлении, одним из наиболее перспективных путей решения проблемы адекватной оценки защищенности ОИ является синтез системы характеристик процессов обеспечения защиты информации на ОИ в рамках соответствующей целевой функции.

В качестве примера такой системы рассмотрим систему характеристик эффективности мер реагирования на угрозы безопасности электронного банкинга [6].

В основу синтеза данной системы положен принцип идентичности структуры системы характеристик эффективности такого рода мер иерархическому представлению функциональной модели процессов реагирования на угрозы безопасности электронного банкинга. В свою очередь функциональная модель процессов реагирования на такого рода угрозы строится на основе функциональной модели противоправных действий в отношении сервисов дистанционного банковского обслуживания (ДБО), а та, в свою очередь, на основе концептуальной модели нарушителя.

В этих условиях модель нарушителя интерпретируется как модель противоправных действий в отношении сервисов ДБО. При этом основными ограничениями на интерпретацию данной модели являются:

1) подобного рода противоправные действия есть способ реализации угроз безопасности электронного банкинга;

2) источником угроз является злоумышленник;

3) для такого рода источника характерно однократное (за исследуемый период) воздействие на среду ДБО;

4) однократное воздействие на среду ДБО осуществляется также из соображений скрытности;

5) нарушение безопасности электронного банкинга связано с проведением соответствующих противоправных действий, связанных со следующими операциями:

- получением конфиденциальной информации клиентов банка;
- модификацией, либо уничтожением этой информации;
- блокированием информационного обеспечения среды ДБО при определенных обстоятельствах.

При этом целевую мотивацию имеют противоправные действия по модификации, либо уничтожению информации клиентов банка.

Соответствия между композиционными признаками группирования состояний функциональной модели процессов реагирования на угрозы безопасности электронного банкинга, композиционными признаками группирования состояний функциональной модели противоправных действий в отношении сервисов ДБО и классификационными основаниями синтезируемой системы характеристик приводятся в таблице 2, а структура самой системы – на рис. 1.

Таблица 2

Соответствие композиционных оснований функциональных моделей исследуемых процессов классификационным основаниям системы характеристик эффективности мер реагирования на угрозы безопасности объектов информатизации

Композиционный уровень	Композиционные основания группирования состояний функциональных моделей		Классификационные основания системы характеристик эффективности мер реагирования
	противоправных действий в отношении сервисов ДБО	процессов реагирования на угрозы безопасности электронного банкинга	
1	Проявление признаков противоправных действий	Выявление признаков противоправных действий	Возможности по выявлению признаков противоправных действий
2	Этапы проведения мошеннической операции в отношении сервисов ДБО	Определение этапов противоправных действий	Возможности по определению этапов противоправных действий
3	Противоправные действия в отношении конкретных сервисов	Установление сервисов ДБО, подверженных угрозам безопасности	Возможности по установлению сервисов ДБО, подверженных угрозам безопасности
4	Целевая функция противоправных действий	Целевая функция мер реагирования	Эффективность мер реагирования на угрозы безопасности электронного банкинга



Рис. 1. Структура системы характеристик эффективности мер реагирования на угрозы безопасности электронного банкинга

С учетом того, что реализация функций реагирования на действия злоумышленника является реакцией на противоправные действия, при формировании характеристик своевременности реагирования на такого рода угрозы условиями своевременного реагирования являются [7]:

$$t_{(y)} < t_{(o)}, \quad (1)$$

$$t_{(o)} < t_{(y)} + \tau_{(y)}, \quad (2)$$

$$t_{(o)} + \tau_{(o)} \leq t_{(y)} + \tau_{(y)}, \quad (3)$$

где: $t_{(y)}$ – момент времени начала проявления угрозы, $\tau_{(y)}$ – время реализации угрозы, $t_{(o)}$ – момент времени обнаружения угрозы, $\tau_{(o)}$ – время реагирования на угрозу. При этом адекватность оценки величин $\tau_{(y)}$ и $\tau_{(o)}$ обеспечивается системным характером механизма оценки.

С учетом случайного характера величин, составляющих условия (1) - (3), выражение для характеристики своевременности E реагирования на угрозы безопасности электронного банкинга может быть представлено в виде вероятности:

$$E = P(t_{(y)} < t_{(o)}, t_{(o)} < t_{(y)} + \tau_{(y)}, t_{(o)} + \tau_{(o)} \leq t_{(y)} + \tau_{(y)}). \quad (4)$$

Таким образом, очевидно, что способ оценки защищенности ОИ путем систематизации и моделирования характеристик процессов обеспечения защиты информации на этих объектах и лишен недостатков характерных оценке защищенности ОИ на основе сертификационных испытаний.

Вывод

Способ оценки защищенности объектов информатизации на основе сертификационных испытаний обладает рядом существенных недостатков, которые могут быть устранены при использовании предложенного подхода к получению этой оценки с помощью математического моделирования. Данный способ позволяет получить адекватную оценку эффективности защиты информации на ОИ в широком диапазоне изменения параметров угроз безопасности информации и применяемых механизмов защиты.

Литература

1. Информационная безопасность телекоммуникационных систем (технические вопросы): учебное пособие для системы высшего профессионального образования России / И.В. Новокшанов, С.В. Скрыль [и др.]. – М.: Радио и связь, 2004. – 388 с.

2. Информационная безопасность открытых систем: учебник для вузов. В 2-х томах. Том 1 – Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: Горячая линия-Телеком, 2006. – 536 с.

3. Основы информационной безопасности: учебное пособие для вузов / Е.Б. Белов, В. П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.

4. Основы системного анализа в защите информации: учебное пособие для студентов высших учебных заведений. / А.А. Шелупанов, С.В. Скрыль. – М.: Машиностроение, 2008. – 138 с.

5. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. - М.: Радио и связь, 2012. - 192 с.

6. Сычев А.М. Система характеристик безопасности электронного банкинга: монография. – М.: ООО «Научтехлитиздат», 2017. – 154 с.

7. Математические модели показателя своевременности реагирования на угрозы безопасности информации для различных моделей ее нарушения / А.М. Сычев, И.Н. Шайков, Т.В. Мещерякова, С.С. Никулин, А.В. Щербаков // Приборы и системы. Управление, контроль, диагностика. – М.: «Научтехлитиздат», 2017. – №81. – С. 14 – 20.

Научный консультант: Скрыль Сергей Васильевич, профессор, д.т.н., профессор кафедры ИУ10 МГТУ им. Н.Э. Баумана, email: zi@bmstu.ru.

ESTIMATION OF SECURITY OF OBJECTS OF INFORMATIZATION ON THE BASIS OF MATHEMATICAL SIMULATION AS AN ALTERNATIVE TO CERTIFICATION TESTING

Sychev M. A.³⁵¹, Sukhorukova N.A.³⁵², Cold D.A.³⁵³

This article shows the possibility of obtaining a numerical evaluation of the security of information objects with the use of mathematical modeling of information security threats, caused by illegal actions, and processes for responding to such actions. This approach will allow to evaluate the effectiveness of the various responses and on the basis of these assessments to justify the most effective system for ensuring security of objects of Informatization.

Keywords: information objects, mathematical modeling, information security, assessment of security certification tests

³⁵¹ Sychev Artem, Ph.D., Associate Professor, Bauman Moscow State Technical University, Moscow, zi@bmstu.ru

³⁵² Sukhorukova Nadezhda, Moscow State Technical University, Moscow, zi@bmstu.ru

³⁵³ Cold Denis Aleksandrovich, Moscow State Technical University, Moscow, zi@bmstu.ru