УДК 004.056.53

ПРОБЛЕМЫ ВЫБОРА ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕХНИЧЕСКОМ ЗАДАНИИ

Екатерина Олеговна Самчук
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, обучающийся кафедры информационной безопасности, тел. (951)389-83-28, e-mail: fsh.rr.n@gmail.com

Виктор Евгеньевич Антипов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, обучающийся кафедры информационной безопасности, тел. (999)462-17-50, e-mail: safe_town@mail.ru

Валентин Валерьевич Селифанов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности, тел. (923)247-25-81, e-mail: sfo1@mail.ru

В данной статье поднимается проблема выбора показателей, которые отвечают за эффективность защиты информации в техническом задании. Рассматривается вопрос насколько выбранное средство защиты подходит для решения конкретных задач, связанных с защитой информации. Также выдвигается предположение об использовании в техническом задании показателей эффективности, которые носят вероятностный характер.

Ключевые слова: техническое задание, показатели, эффективность, средства защиты информации

PROBLEMS OF SELECTING INFORMATION SECURITY PERFORMANCE INDICATORS IN THE TERMS OF REFERENCE

Ekaterina O. Samchuk
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Student, Department of Information Security, phone: (951)389-83-28, e-mail: fsh.rr.n@gmail.com

Viktor E. Antipov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Student, Department of Information Security, phone: (999)462-17-50, e-mail: safe_town@mail.ru

Valentin V. Selifanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Associate Professor of the Department of Information Security, phone: (923)247-25-81, e-mail: sfo1@mail.ru

This article raises the problem of selecting indicators that are responsible for the effectiveness of information protection in the terms of reference. The question of whether the chosen security tool is suitable for specific tasks related to the protection of information is considered. It also suggests the use of performance indicators in the terms of reference, which are probabilistic in nature.

Keywords: terms of reference, indicators, efficiency, information security tools

Введение

Ни для одного специалиста в области информационной безопасности не секрет, что существуют множество факторов, будь то внешние или внутренние, воздействие которых может повлиять на обеспечение защиты информации в информационной системе.

Требования к системе защиты информации информационной системы включаются в техническое задание (ТЗ), которое является обязательным документом, и которое должно быть разработано в соответствии с национальными стандартами, нормативными и методическими документами. Но помимо требований к системе, существуют требования к мерам и средствам защиты информации (СЗИ), которые применяются в информационной системе, и они, в свою очередь, достаточно высоки, т.к. внедряемые средства должны иметь лицензии, сертификации ФСТЭК и ФСБ и т.д.

Несертифицированное или нелицензированное средство может подвести в любой момент и вывести из функционирования всю систему безопасности системы, что повлечет за собой финансовые убытки. Еще более опасно, если несертифицированное или нелицензированное средство защиты информации установлено в государственной информационной системе или на значимом объекте критической информационной инфраструктуры, так как это может привести к штрафным санкциям.

Но при всей важности этих требований нет ответа на один из насущных вопросов – насколько то или иное выбранное решение подходит для конкретного спектра задач, и какова его эффективность в реалиях заданной информационной системы.

Методы и материалы

Итак, техническое задание разрабатывается в соответствии с ГОСТ 34.602-89 «Техническое задание на создание автоматизированной системы», ГОСТ Р 51624-2000 «Автоматизированные системы в защищенном исполнении», ГОСТ Р 51583-2014 «Порядок создания автоматизированных систем в защищенном исполнении», Приказом ФСТЭК России №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», методическими документами «Профили защиты», а также «Меры защиты в ГИС», если это государственная информационная система. Данные документы содержат в себе требования для создания самого технического задания, системы ЗИ и средств ЗИ.

Результаты

В ГОСТе 34.602-89, а конкретно в пункте 2.12 говорится об эффективности, а именно о включении приложений, содержащих расчет ожидаемой эф-

фективности системы, в состав технического задания. Об эффективности упоминается и в ГОСТе Р 51624-2000, цели защиты информации в АСЗИ должны включать показатель эффективности достижения цели и требуемое его значение. Из ГОСТа Р 50922-96 «Защита информации» следует, что характеристики эффективности защиты информации должны носить вероятностный характер, а значит ее оценка обязательно должна учитывать объективные обстоятельства.

Расчет эффективности предполагает решение следующих задач:

– во–первых, приемлемость использования СЗИ на практике в реальной ситуации, т.е. в какой степени выбранное нами СЗИ подойдет для решения задач защиты информации в конкретной информационной системе;

– во–вторых, сравнение схожих вариантов систем, которые будут обеспечивать защиту ИС.

Выявление путей повышения эффективности СЗИ также является решаемой задачей при расчете общей эффективности системы защиты. Ну и диагностирование прочих факторов и их вкладов в достижение цели, что позволит нам в полной мере понять, от чего зависит защищенность той или иной системы.

Поэтому именно вероятность, при данных условиях, может выступать в роли объективной характеристики качества СЗИ. Данная характеристика будет назваться вероятностью достижения цели или же вероятностью достижения задачи. В основу перечня показателей и критериев оценки эффективности должна быть положена такая вероятность.

Тогда пригодность и оптимальность могут выступать критериями оценки (табл. 1).

Таблица 1

Потенциальные критерии эффективности СЗИ

Концепция эффективности СЗИ	Критерии эффективности
Оптимальность	Наилучший результат
	Наилучший средний результат
	Наибольшая вероятность гарантии результата
	Наибольший гарантированный результат
Пригодность	Приемлемый результат
	Допустимая гарантия
	Допустимый гарантированный результат

Пригодность означает выполнение всех предусмотренных требований к СЗИ, а оптимальность – достижение одной из характеристик экстремального значения с учетом соблюдения ограничений и условий других особенностей системы, показатели эффективности СЗИ представлены в табл. 2.

Таблица 2

Показатели эффективности СЗИ

Требования к СЗИ	Вид показателя эффективности
Наступление или отсутствие события	Вероятность события
Достижение требуемых характеристик	Вероятность достижения результата не ниже требуемого уровня
Не установлены	Математическое ожидание результата
	Дисперсия результата
	Средний риск
Отклонение от заданных характеристик	Средний квадрат отклонения результата от требуемого значения
Обеспечение гарантированного уровня характеристик	Квантиль заданного уровня гарантии

Обсуждение

Немалая часть авторов берут во внимание показатели эффективности, предназначенные для задач сравнения структур СЗИ.

Также существуют показатели вероятностно-временного характера, работающие по принципу функций распределения. Как пример – это вероятность преодоления системы защиты информации за определенное время.

Классификационный подход является популярным для современных нормативных документов по информационной безопасности, но, несмотря на то, что вероятностные методы выглядят более конструктивными, они нашли широкое применение в других прикладных областях обеспечения безопасности.

Опираясь на эти методы, уровни гарантий безопасности СЗИ переходят в так называемые доверительные вероятности оценок. Чтобы решить эту задачу, рекомендуется использовать статистическую теорию решений, которая позволит найти оптимальные уровни гарантий безопасности.

Заключение

Включаемые в ТЗ СЗИ, без сомнения, обязаны гарантировать требуемую степень безопасности, для этого потребуется оценить эффективность СЗИ, проводить оценку следует показателями, носящими вероятностный характер.

Нормативная база, а также методические документы в области информационной безопасности, должны совершенствоваться именно в данном направлении.

Системный подход выделяет содержательные результаты, если использовать его при оценке эффективности системы защиты. В свою очередь, количественная оценка подразумевает большие усилия при работе с эффективностью СЗИ, нежели используемые качественные методы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Баутов А. Экономический взгляд на проблемы информационной безопасности. Открытые системы. 2002. [Электронный ресурс]. URL: https://www.osp.ru/os/2002/02/034.htm (дата обращения: 15.04.2021).

2. Баутов А. Эффективность защиты информации. 2003. [Электронный ресурс]. URL: https://www.osp.ru/os/2003/07-08/183282 (дата обращения: 15.04.2021).

3. Горбунов А., Чуменко В., Выбор рациональной структуры средств защиты информации в АСУ [Электронный ресурс]. URL: http://kiev-security.org.ua/box/2/26.shtml (дата обращения: 16.04.2021).

4.ГОСТ Р 51624-2000. Автоматизированные системы в защищенном исполнении [Электронный ресурс]. URL: http://www.fa.ru/org/div/uank/Documents/2051624-2000.pdf (дата обращения: 16.04.2021).

5. ГОСТ Р 50922-96. Защита информации [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200004674 (дата обращения: 17.04.2021).

6. ГОСТ Р 51583-2014. Порядок создания автоматизированных систем в защищенном исполнении [Электронный ресурс]. URL: https: // files.stroyinf.ru / Index2 /1/4293772/4293772843.htm (дата обращения: 13.04.2021).

7. ГОСТ 34.602-89. Техническое задание на создание автоматизированной системы [Электронный ресурс]. URL: https://meganorm.ru/Index2/1/4294850/4294850134.htm (дата обращения: 17.04.2021).

8. Документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации [Электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty (дата обращения: 16.04.2021).

9. Методический документ ФСТЭК России. Меры защиты информации в государственных информационных системах [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200004674 (дата обращения: 17.04.2021).

10. Приказ ФСТЭК России №17. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. [Электронный ресурс]. URL: https://fstec.ru/component/attachments/download/566 (дата обращения: 13.04.2021).

11. Щуровская А.Ю., Унтилов А.М. Критерии и показатели эффективности защиты информации [Электронный ресурс]. URL: http://www.rusnauka.com/10_NPE_2010/ Informatica/62689.doc.htm (дата обращения: 12.04.2021).