Оригинальная статья/Original article

УДК 004.056.52

DOI: http://doi.org/10.20914/2310-1202-2017-2-107-112

Формализация анализа уязвимостей информационной системы при проектировании КСЗИ

И.Е. Грабежов [1]
Ю.А. Леонов [1]

[1] Брянский государственный технический университет, бул. 50-лет Октября, 7, г. Брянск, 241035, Россия

Реферат. Информационные системы и технологии, как компоненты информационной сферы, непосредственно и активно влияют на состояние экономической, экологической, энергетической, транспортной, продовольственной, криминогенной, информационной и других составляющих комплексной безопасности РФ. В статье рассматриваются вопросы формализации параметров информационной системы, от которых зависит значение информационных рисков. Приводится методика проектирования комплексных систем защиты информации путем разделения на соответствующие этапы. С помощью разработанного ПО проектируется КСЗИ на основе объективных параметров информационной системы. Модель представляет собой совокупность объектов информационной системы, описанных при помощи соответствующих программных сущностей. Это позволяет повысить точность расчетов, избежать зависимости от опыта экспертов, что, в конечном итоге, позволит использовать ПО системным администраторам, не имеющим большого опыта в проектировании систем защиты

Ключевые слова: система защиты информации, информационный риск, угроза информационной безопасности, уязвимость информационной системы

Formalization of the analysis of the vulnerabilities of the information system in the design of KSZI

I.E. Grabezhov [1]
Ju.A. Leonov [1]

[1] Bryansk State Technical University, Bulvar 50-letiya Oktyabrya, 7, Bryansk, 241035, Russia

Summary. Information systems and technologies, as components of the information sphere, directly and actively influence the state of economic, ecological, energy, transport, food, criminogenic, information and other components of the integrated security of the Russian Federation. The article deals with the formalization of the information system parameters, on which the importance of information risks depends. The technique of designing complex information security systems is described by dividing them into appropriate stages. With the help of the developed software, the KSZI is designed on the basis of the objective parameters of the information system. The model is a set of objects of the information system, described with the help of appropriate software entities. This allows you to improve the accuracy of calculations, avoid dependence on the expertise of experts, which ultimately will allow the software to be used by system administrators who do not have much experience in designing security systems.

Keywords: information security system, information risk, information security threat, vulnerability of the information system

Введение

В Доктрине информационной безопасности Российской Федерации настоящий этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации.

Информационные системы (ИС) и технологии, как компоненты информационной сферы, непосредственно и активно влияют на состояние экономической, экологической, энергетической, транспортной, продовольственной, криминогенной, информационной и других составляющих комплексной безопасности РФ.

Информационные системы являются одним из системообразующих факторов жизни современного общества, и их влияние на все стороны жизни общества с течением времени будет только возрастать.

Информация, находящаяся в ИС, подвержена множеству угроз, а работа информационной системы – множеству дестабилизирующих факторов. Источниками угроз и дестабилизирующих факторов могут являться ошибки пользователей, недокументированные возможности программного обеспечения, ненадёжность аппаратуры и т. д. Развитие информационных технологий позволяет предоставить пользователю всё больше сервисов, однако приводит к усложнению ИС и снижению её надёжности. В условиях жёсткой конкурентной борьбы возрастает риск целенаправленного воздействия на информацию и информационную систему со стороны конкурентов, криминальных структур и других злоумышленников.

Приведённые выше причины, заставляют обращать большое внимание на обеспечение информационной безопасности ИС. При этом, решение частных задач защиты информации не обеспечивает должного уровня информационной

Для цитирования

Грабежов И.Е., Леонов Ю.А. Формализация анализа уязвимостей информационной системы при проектировании КСЗИ // Вестник ВГУИТ. 2017. Т. 79. № 2. С. 107–112. doi:10.20914/2310-1202-2017-2-107-112

For citation

Grabezhov I.E., Leonov Ju.A. Formalization of the analysis of the vulnerabilities of the information system in the design of KSZI. *Vestnik VGUIT* [Proceedings of VSUET]. 2017. vol. 79. no. 2. pp. 107–112. (in Russian). doi:10.20914/2310-1202-2017-2-107-112

безопасности. Защита информации должна производиться комплексно, что требует построение *комплексных систем защиты информации* (*КСЗИ*).

В процессе эксплуатации информационной системы, например, при её изменении или изменении условий работы системы также необходимо изменять и систему защиты. Поэтому проектирование или доработку КСЗИ необходимо производить в течении всего жизненного цикла ИС.

Процесс проектирования КСЗИ можно условно разделить на четыре этапа:

1. Анализ информации, циркулирующий в информационной системе.
2. Анализ угроз информационной безопасности.
3. Разработка организационно-технических мероприятий по защите информации.
4. Анализ эффективности разработанной КСЗИ.

1 Этап. Анализ информации, циркулирующей в системе | **Stage 1.** Analysis of information circulating in the system
1.1 Определение состава защищаемой информации | 1.1 Determination of the composition of the protected information
1.2 Оценка стоимости защищаемой информации | 1.2 Estimation of the cost of the protected information
2 Этап. Анализ угроз информационной безопасности | **2 Stage.** Analysis of information security threats
2.1 Определение множества угроз информационной безопасности | 2.1 Identifying a variety of information security threats
2.2 Оценка угроз информационной безопасности | 2.2 Assessing Information Security Threats
2.3 Определения множества уязвимостей информационной системы 2.3 Definitions of the Multiple Vulnerabilities of the Information System
2.4 Оценка уязвимостей информационной системы | 2.4 Assessing the vulnerabilities of the information system
2.5 Расчет информационных рисков | 2.5 Calculation of information risks
3 Этап. Разработка мероприятий по защите информации | **3 Step.** Development of measures to protect information
3.1 Разработка организационных мероприятий | 3.1 Developing Organizational Measures
3.2 Подбор технических средств | 3.2 Selection of technical means
4 Этап. Анализ эффективности, разработанной КСЗИ | **4 Stage.** Analysis of the effectiveness of the CCIS

Рисунок 1. Этапы проектирования КСЗИ

Figure 1. Stages of designing KSZI

Каждый этап условно разбивается на подэтапы (рисунок 1). На первом этапе производится анализ информации, циркулирующий в ИС. Определяются основные информационные активы (ИА), подлежащие защите, их стоимость (C_{au}), а также необходимый уровень защиты. Данный этап проводиться с обязательным участием владельцев информации, поскольку только они могут определить, насколько важен для них тот или иной информационный актив [1].

После оценки стоимости информации владельцам необходимо определиться с величиной максимально допустимого информационного риска (R_{max}). Как показывает практика, невозможно обеспечить абсолютную защиту информации. Всегда остаётся определённая вероятность воздействия угрозы на информацию. Поэтому при проектировании КСЗИ необходимо определиться с величиной риска, который останется после применения всех средств защиты информации. Косвенно данная величина определяет необходимый уровень информационной безопасности.

Анализ угроз информационной безопасности производится на втором этапе. Он включает: определение множества угроз и оценку вероятности их проявления, определение множества уязвимостей и оценку вероятности реализации угроз, посредством этих уязвимостей, а также анализ информационных рисков.

Множество угроз информационной безопасности определяется группой экспертов. В данную группу должны входить специалисты по защите информации и владельцы информации. Значение вероятности ($P_{уг}$) угроз можно определить исходя из статистических данных, если они есть, или на основе мнений специалиста [1].

Множество уязвимостей информационной системы и вероятность ($P_{уз}$) их проявления определяются на основе свойств самой системы и условий её эксплуатации. На практике, эти параметры также определяются экспертами.

Основная часть

Информационные риски можно рассчитать исходя из формулы:

$$R = C_{au} \cdot P_{уг} \cdot P_{уз}, \qquad (1)$$

где C_{au} – стоимость актива; $P_{уг}$ – вероятность угрозы; $P_{уз}$ – вероятность уязвимости.

В государственных стандартах, регламентирующих методы и средства безопасности, [3] риску даётся следующее определение: «…потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов. Определяется как сочетание

вероятности события и его последствий». В самом простом виде риск можно понимать, как то чем рискует владелец информации при реализации угрозы. При более внимательном рассмотрении понятия информационного риска становится очевидным, что это комплексная величина. Она показывает возможные потери при реализации угроз, вероятность угрозы, значение уязвимости актива. Анализ рисков информационной безопасности проявляет важность актива для владельца, наиболее вероятные угрозы и наиболее опасные уязвимости. Поэтому, при проектировании КСЗИ, анализ рисков становиться самым важным для обоснования последующих решений.

На третьем этапе определяются мероприятия по защите информации. Мероприятия по защите выбираются так, чтобы противодействовать угрозам информационной безопасности. Очевидна прямая связь между объектами ИС, реализующими ИА, мерами защиты, уязвимостями и угрозами. Угроза информационной безопасности воздействует на информационный актив посредством уязвимости информационной системы. Эта взаимосвязь наглядно показана на схеме модели защиты с полным перекрытием (рисунок 2). Мероприятия по защите информации необходимо подбирать так, чтобы нейтрализовать уязвимость.

Полная или частичная нейтрализация уязвимости снижает величину реального информационного риска. Если величина риска, рассчитанная при проектировании выше величины максимально допустимого, то необходимо применять мероприятия по защите информации.

$$R > R_{\max} \qquad (2)$$

Для обеспечения принятых мер информационной безопасности подбираются технические средства. Совокупность разработанных мероприятий и подобранных технических средств определяет содержимое проекта КСЗИ.

На четвёртом этапе производится оценка эффективности принятых мер. Для этого необходимо заново пересчитать значения реальных рисков. При пересчёте учитывается снижение вероятности уязвимости, а также увеличение стоимости ИА. Это происходит потому, что мероприятия по защите информации снижают степень воздействия угрозы на актив с одной стороны, но требуют увеличения затрат – с другой. Если, после принятых мер, риск информационной безопасности остаётся выше максимально допустимого (2), то необходимо, либо принять дополнительные меры, либо изменить принятые. КСЗИ должна обеспечить снижение уровня реального риска по отношению к максимально допустимому. Так обеспечивается заданный уровень информационной безопасности.

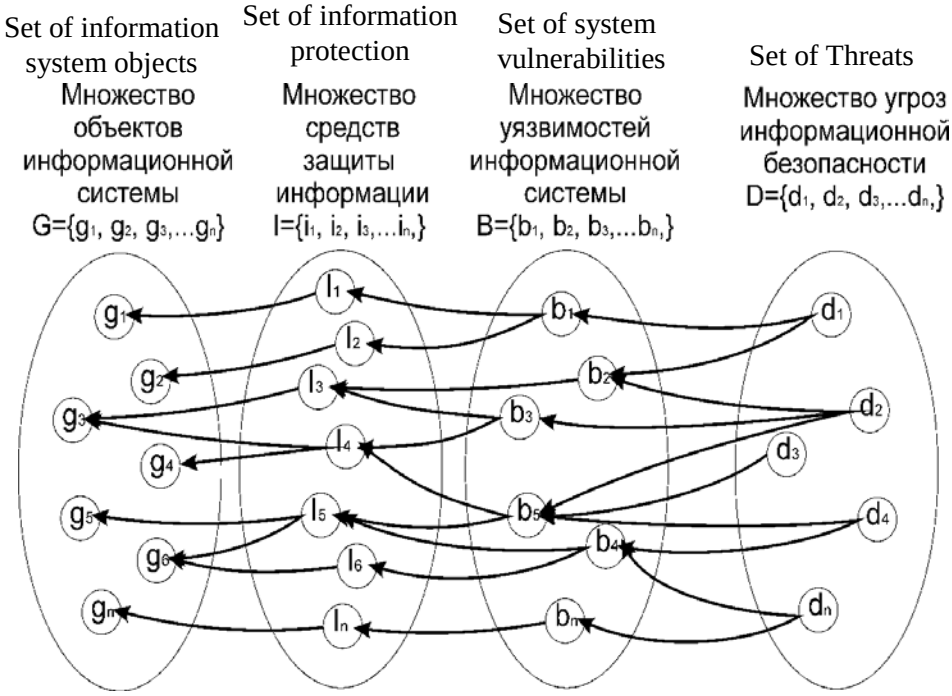

Рисунок 2. Модель защиты информации с полным перекрытием угроз

Figure 2. The model of information security with full overlap of threats

Процесс проектирования КСЗИ является сложным и трудоёмким. В ходе проектирования приходится решать множество слабоформализуемых задач. Все параметры, на основе которых производится расчет, получаются методом экспертных оценок. Такое положение приводит к снижению точности расчётов, зависимости от квалификации и опыта экспертов, повышает стоимость проекта. Автоматизация проектирования КСЗИ позволяет снизить трудоемкость и время проектирования. Автоматизированный учет большого количества параметров позволяет избежать ошибок при их анализе.

Исходя из свойств информации, как объекта защиты, исключить мнение экспертов и владельцев информации из оценки стоимости ($C_{аи}$) и вероятности угрозы ($P_{уг}$) невозможно. Однако третий ключевой параметр формулы (1) – вероятность проявления уязвимости ИС, принципиально, можно оценить на основе параметров информационной системы. Так, формализация анализа оценки вероятности уязвимости информационной системы является одной из основных задач автоматизации проектирования КСЗИ.

В стандарте [3] уязвимость информационной системы определяется, как слабость ИА, которая может быть использована одной или несколькими угрозами. Такое определение даёт возможность предположить, что вероятность реализации угрозы через конкретную уязвимость зависит от параметров ИС. В большинстве случаев эти параметры являются физическими величинами, например: техническими характеристиками аппаратуры или величинами, такими как напряжение питания, температура окружающей среды и т. д. Также эти параметры могут не являться физическими величинами, но выражаться в числовом виде, например, квалификацию пользователей системы можно выразить в периоде его работы или оценкой, полученной при сдаче зачёта при повышении квалификации.

Любую информационную систему можно представить в виде совокупности её элементов – объектов системы. Каждый объект характеризуется множеством параметров. Например, файл характеризуется его размером, типом, адресом, по которому он хранится на диске. Совокупность всех параметров всех объектов составляет множество параметров ИС. Совокупность текущих значений этих параметров характеризует состояние системы.

Пусть множество Q описывает все возможные состояния системы, а множество X – множество всех параметров системы, тогда отношение $M : Q \times X$ описывает все состояния системы значениями её параметров, а каждому элементу $q \in Q$ соответствует некоторая композиция (x_1, x_2, $x_3 \ldots x_n$.) значений параметров. Реализация уязвимости в информационной системе соответствует определённому состоянию этой системы $q_{\text{Bn}} \in Q$. Данному состоянию также соответствует композиция значений параметров $X_{Bn}(x_1, x_2, x_3 \ldots x_n.)$. Это означает, что множество уязвимостей B соответствует множеству определённых состояний системы Q_B, такому что ($Q_B \subset Q$), каждому из которых соответствует своя композиция значений параметров системы. Таким образом, можно утверждать, что множество уязвимостей является отношением M_B: $Q_B \times X_B$, а числовое значение вероятности зависит от композиции значений параметров:

$$P_{уз} = F(X) \qquad (3)$$

Конкретная зависимость вероятности реализации уязвимости от значений параметров системы на практике определяется исходя из свойств информационной системы и условий её функционирования.

Для разработки КСЗИ необходимо получить экспертную оценку стоимости информационных активов – $C_{иа}$, вероятности реализации угроз – $P_{уг}$, а также задать максимально допустимый уровень риска R_{max}. При этом, исходя из формулы (1) можно рассчитать значения вероятностей реализации уязвимости ($P_{уз\,i}$) для каждого ИА по каждой угрозе, при которых информационные риски будут равны максимально допустимым.

$$P_{узi} = \frac{R_{\max}}{P_{уг\,\text{n}} C_{ИА\,\text{k}}}, \qquad (4)$$

где R_{max} – максимально допустимый информационный риск, $P_{уг\,n}$ – вероятность n-ой угрозы, $C_{ИА\,k}$ – стоимость k-*го* ресурса.

После этого, исходя из формулы (3), можно рассчитать значения для каждого параметра ИС. Это будут «граничные» значения, т. е. значения, за пределы которых система выходить не должна. В противном случае возрастает риск или появляется возможность реализации угрозы. КСЗИ для данной системы должна состоять из мероприятий, позволяющих удержать значения параметров ИС в пределах граничных значений.

Для реализации системы автоматизированного проектирования КСЗИ было разработано программное обеспечение (ПО). В основе ПО лежит программная реализация: объектов ИС, уязвимостей ИС, мероприятий по защите ИС. Основными элементами ПО являются множество параметров и множество зависимостей.

Функциональная схема программы представлена на рисунке 3. При проектировании системы защиты информации, оператор формирует модель ИС. Модель представляет собой совокупность объектов информационной системы, описанных при помощи соответствующих программных сущностей.

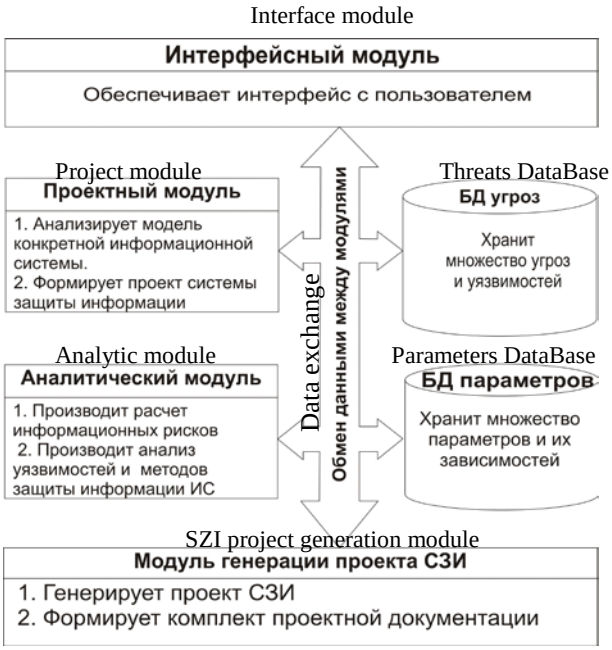

Рисунок 3. Функциональная схема программного комплекса проектирования КСЗИ

Figure 3. Functional diagram of the software complex of the KSZI design

Для модели ИС формируется множество возможных угроз информационной безопасности и множество уязвимостей. С каждой угрозой связана одна или несколько уязвимостей ИС, а также объекты ИС, для которых характерны эти уязвимости. Далее, производится расчет информационных рисков для модели ИС. Затем разрабатываются мероприятия по защите.

Множество угроз и уязвимостей хранится в отдельной базе данных и может использоваться повторно при разработке других проектов. Модель ИС, множество угроз и уязвимостей формируется в «Проектном модуле». Параметры объектов информационной системы и уязвимостей сохраняются в соответствующей базе данных (рисунок 3) – «БД параметров». Расчет рисков производит «Аналитический модуль».

Если для защиты информации необходимо применение технических средств, то такие средства становятся дополнительными объектами в модели. В ином случае – они изменяют свойства существующего объекта, т. е. меняют его параметры. Модель ИС изменяется за счёт добавления новых объектов и изменения параметров. После изменения модели производится повторный анализ в «Аналитическом модуле».

Процесс проектирования КСЗИ заканчивается, когда величина рисков не превышает максимально допустимые значения. После этого производится генерация проекта в виде перечня мероприятий и списка используемых средств защиты информации.

Заключение

С помощью разработанного ПО проектируется КСЗИ на основе объективных параметров ИС. Это позволяет повысить точность расчетов, избежать зависимости от опыта экспертов, что, в конечном итоге, позволит использовать ПО системным администраторам, не имеющим большого опыта в проектировании систем защиты.

ЛИТЕРАТУРА

1 Аверченков В.И., Рытов М.Ю., Кувыклин А.В., РудановскийМ.В. Аудит информационной безопасности органов исполнительной власти. Москва. Флинта, 2011. 100 с.

2 Whitman M. E., Mattord H. J. Principles of information security. Cengage Learning, 2011.

3 ГОСТ Р ИСО 13335-1-2006 Информационные технологии. Методы и средства обеспечения безопасности

4 Ifinedo P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory // Computers & Security. 2012. Т. 31. №. 1. С. 83-95.

5 Казаков Ю.М., Леонов Ю.А., Федоров В.Е. Моделирование рациональных схем базирования заготовки при решении задачи синтеза единичных технологических процессов // XI Международная научно-практическая конференция "Михаило-Архангельские чтения". 2016. С. 203–235.

6 Тищенко А.А., Казаков Ю.М. Методика принятия решений о производстве нового изделия на начальных этапах разработки при маркетинговом подходе управления // Вестник Славянских вузов: ежегодный международный научно-практический журнал. 2015. № 4. С. 127–130.

7 Аверченков А.В., Фисун А.П. Модель многоуровневой идентификации персонала в системе контроля и управления доступом на предприятиях строительной индустрии // Строительство и реконструкция. 2016. № 2. С. 56–64.

8 Tankard C. Advanced persistent threats and how to monitor and deter them // Network security. 2011. Т. 2011. №. 8. С. 16-19.

REFERENCES

1 Averchenkov V.I., Rytov M.Yu., Kuvyklin A.V., Rudanovskii M.V. Audit informatsionnoi bezopasnosti organov ispolnitel'noi vlasti [Information security audit of the Executive bodies]. Moscow. Flinta 2011. 100 p. (in Russian).

2 Whitman M. E., Mattord H. J. Principles of information security. Cengage Learning, 2011.

3 GOST no. 13335-1-2006. Informatsionnye tekhnologii. Metody i sredstva obespecheniya bezopasnosti [State standard no. 13335-1-2006. Information technology. Methods and means of security]. (in Russian).

4 Ifinedo P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*. 2012. vol. 31. no. 1. pp. 83-95.

5 Kazakov Yu.M., Leonov Yu.A., Fedorov V.E. Modeling rational schemes of basing of the workpiece in the solution of the problem of synthesis of individual technological processes. XI Mezhdunarodnaya nauchno-prakticheskaya konferentsiya "Mikhailo-Arkhangel'skie chteniya". 2016. pp. 203–235. (in Russian).

6 Tishchenko A.A., Kazakov Yu.M. The method of decision-making about the production of a new product in the initial stages of development at the marketing management approach. *Vestnik Slavyanskikh vuzov: ezhegodnyi mezhdunarodnyi nauchno-prakticheskii zhurnal* [Journal of Slavic universities: the annual international scientific-practical journal]. 2015. no. 4. pp. 127–130. (in Russian).

7 Averchenkov A.V., Fisun A.P. A multilevel model of personnel identification in the control system and access control at the enterprises of construction industry. *Stroitel'stvo i rekonstruktsiya* [Construction and reconstruction]. 2016. no. 2. pp. 56–64. (in Russian).

8 Tankard C. Advanced persistent threats and how to monitor and deter them. *Network security*. 2011. vol. 2011. no. 8. pp. 16-19.

СВЕДЕНИЯ ОБ АВТОРАХ

И.Е. Грабежов к.т.н., доцент, кафедра компьютерные технологии и системы, Брянский государственный технический университет, бул. 50-лет Октября, 7, г. Брянск, 241035, Россия,

Ю.А. Леонов к.т.н., доцент, кафедра компьютерные технологии и системы, Брянский государственный технический университет, бул. 50-лет Октября, 7, г. Брянск, 241035, Россия,

КРИТЕРИЙ АВТОРСТВА

Все авторы в равной степени принимали участие в написании рукописи и несут ответственность за плагиат

КОНФЛИКТ ИНТЕРЕСОВ

Авторы заявляют об отсутствии конфликта интересов.

ПОСТУПИЛА 13.04.2017

ПРИНЯТА В ПЕЧАТЬ 19.05.2017

INFORMATION ABOUT AUTHORS

I.E. Grabezhov candidate of technical sciences, assistant professor, computer technologies and systems department, Bryansk State Technical University, Bulvar 50-letiya Oktyabrya, 7, Bryansk, 241035, Russia,

Ju.A. Leonov candidate of technical sciences, assistant professor, computer technologies and systems department, Bryansk State Technical University, Bulvar 50-letiya Oktyabrya, 7, Bryansk, 241035, Russia,

CONTRIBUTION

All authors equally took part in writing the manuscript and are responsible for plagiarism

CONFLICT OF INTEREST

The authors declare no conflict of interest.

RECEIVED 4.13.2017

ACCEPTED 5.19.2017