УДК 681.3

Меры по обеспечению безопасности и защиты информации для сложных информационных систем

Осовецкий Л. Г., Суханов А. В., Ефимов В. В.

Постановка задачи: *рост числа компонент информационных систем приводит к росту их сложности и необходимому изменению требований по безопасности и классификации этих требований и мер по обеспечению безопасности в зависимости от уровня сложности информационной системы. Существующие нормативные требования по безопасности и меры по ее обеспечению включают управление доступом, регистрацию и учет, криптографическую подсистему, обеспечение целостности информации. Указанные группы требований не учитывают влияния сложности защищаемой информационной системы на ее безопасность и защищенность.*

Анализ изменения поля угроз безопасности и требований к защите информации показал, что с ростом сложности информационной системы учет числа компонент информационной системы и ее сложности позволят адекватно модифицировать и детализировать необходимые нормативные требования по безопасности, а также классифицировать их в зависимости от метрической сложности информационной системы. Классификация метрической сложности информационных систем по числу компонент дополняет методический аппарат построения защиты, адекватной полю угроз системы безопасности, а также выбор мер по обеспечению безопасности, квалифицированных в зависимости от сложности информационных систем. Обосновывается и предлагается дополнение общих требований по безопасности новой группой требований, которые адекватны уровню сложности информационной системы. ***Целью работы*** *является оценка и анализ влияния метрической сложности информационных систем на их безопасность и защищенность, а также выработка и классификация требований по безопасности к информационным системам по критерию «сложность–безопасность», формулировка классификационных требований и мер обеспечения безопасности с учетом сложности информационной системы. Это позволит обеспечить построение подсистемы безопасности и защиты информации, которая адекватна полю угроз и уровню сложности информационной системы. Предлагается применять требования и меры повышения безопасности информационных систем в соответствии с дополнительной нормативной группой требований – классификацией сложности информационных систем,.* ***Используемые методы****: научно-методический аппарат выбора и классификации требований по безопасности информационной системы, мер и состава их реализации с учетом уровня ее сложности.* ***Новизна:*** *новизной представленного решения является использование при определении нормативных требований по безопасности информационной системы и мер по их реализации, дополнительной группы нормативных требований, учитывающей сложность защищаемой системы.* ***Результат:*** *использование представленного решения по учету влияния сложности защищаемой системы при классификации требований и мер по обеспечению безопасности позволяет снизить уровень угроз безопасности и обеспечить эффективность подсистемы защиты, а также снизить затраты на ее создание и потери от действия угроз безопасности. Моделирование расчетов уровня безопасности ряда сложных информационных систем с учетом сложности этих систем позволило обосновать необходимость усиления мер безопасности для некоторых из них.* ***Практическая значимость:*** *представленное решение предлагается использовать при выборе нормативных требований и мер по безопасности современных сложных информационных систем, аттестации по требованиям безопасности информации сложных объектов информатизации, создании и проектировании*

Библиографическая ссылка на статью:
Осовецкий Л. Г., Суханов А. В., Ефимов В. В. Меры по обеспечению безопасности и защиты информации для сложных информационных систем // Системы управления, связи и безопасности. 2017. № 1. С. 16-25. URL: http://sccs.intelgr.com/archive/2017-01/02-Osovetskiy.pdf

Reference for citation:
Osovetskiy L. G., Sukhanov A. V., Efimov V. V. Measures to Ensure Security and Data Protection for Complex Information Systems. *Systems of Control, Communication and Security*, 2017, no. 1, pp. 16-25. Available at: http://sccs.intelgr.com/archive/2017-01/02-Osovetskiy.pdf

подсистем безопасности сложных информационных систем, оптимизации средств отражения воздействия угроз безопасности.

Ключевые слова: *информационная система, безопасность, защита информации, угрозы безопасности, меры защиты, нормативные требования.*

Введение

Эффективность информационной системы (ИС) в значительной степени зависит от уровня ее безопасности. Опыт эксплуатации ИС показывает, что уровень безопасности и защищенности таких систем не всегда отвечает современным требованиям, поэтому весьма актуальна проблема разработки методов, позволяющих обеспечить необходимые уровни характеристик защищенности и безопасности ИС.

Российские и зарубежные нормативные документы [1, 2, 4, 5, 6, 7] определяют требования по защищенности и безопасности без учета роста сложности ИС, что зачастую приводит по формальным причинам к ошибкам в реализации и проектировании систем защиты и безопасности ИС. К сложным ИС и автоматизированным системам (АС) предъявляются и реализуется тот же уровень требований, что и для простых систем, что приводит к превышению необходимых требований для простых ИС и АС, а также их недостаточности для сложных современных систем [3]. С ростом уровня сложности ИС назрела естественная необходимость классификации требований по безопасности ИС по уровню их сложности.

В основу классификации требований к безопасности с учетом сложности ИС положена существующая классификация АС и ИС по безопасности и защищенности в соответствии с РД ФСТЭК России.

В общем случае, комплекс требований и мер решений по защите информации от несанкционированного доступа (НСД) реализуется в рамках системы защиты информации (СЗИ) от НСД, состоящей из следующих четырех групп требований:

- управления доступом;
- регистрации и учета;
- криптографической защиты;
- обеспечения целостности.

При этом требования по защищенности в первой группе усиливаются от класса 1Д к 1А.

Расчеты, представленные в работе [8], показывают, что при существующем сегодня уровне воздействия угроз безопасности существует оценка по уровню математического ожидания наработки на отказ комплекса сложных ИС и АС в зависимости от их сложности.

Такая градация приведена в таблице 1.

Таким образом, для компенсации роста отказов по причине роста сложности ИС, необходимо изменение требований по безопасности к АС и ИС в сторону их увеличения (таблица 2).

Таблица 1 – Классификация ИС и АС по уровню математического ожидания наработки на отказ и в зависимости от их сложности

Сложность ИС и АС (в количестве рабочих мест)	Математическое ожидание отказа при действии угроз в часах
1	199
10	149
100	20
1000	7

Таблица 2 – Оценка необходимого повышения требуемого класса защищенности ИС с ростом уровня ее сложности

Сложность ИС и АС (в количестве рабочих мест)	Повышение требуемого класса защищенности ИС
1	нет
10	+1
100	+2
1000 и более	+3 и более

К сожалению, данные по вероятности атак на отдельные рабочие места очень разрозненны, а иногда не сходятся или противоречат друг другу. Поэтому, для демонстрации расчетов оценок, воспользуемся примером на базе данных, приведенных на рис. 1.

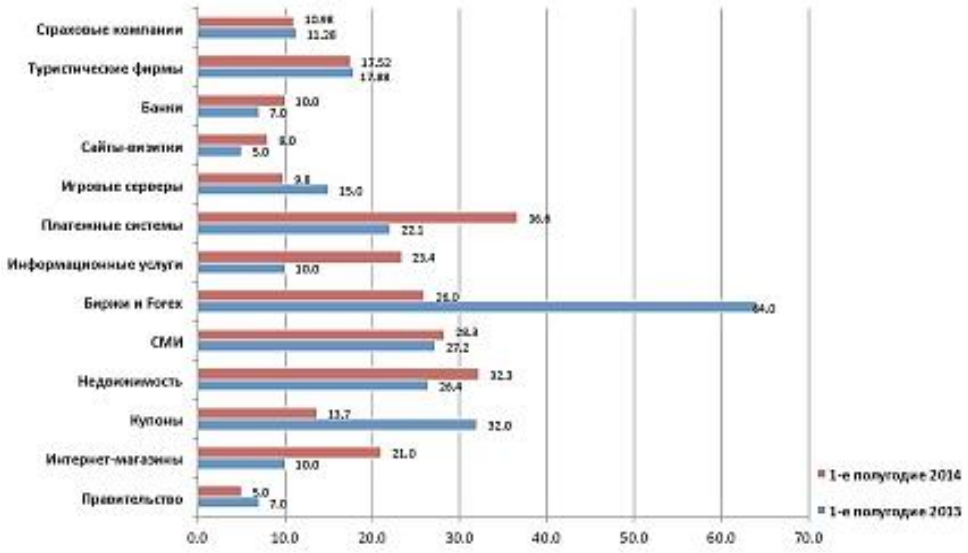

Рис. 1. Пример данных по количеству атак в год на рабочие места ИС

Вероятность действия атак на отдельные рабочие места в год, согласно этим данным, колеблется для ИС различного применения назначения от 0,05 до 0,6. Для демонстрации расчетов введем допущение о том, что среднее значение вероятности атаки на рабочее место ИС равно 0,1.

Далее, примем допущение, что атаки на отдельные рабочие места ИС независимы, тогда по соотношению (1) для вероятности независимых событий можно рассчитать вероятность атак на ИС в целом.

По теореме для вероятности независимых несовместных событий

$$P\left(\sum_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} P(A_i), \quad (1)$$

где: i – количество компонентов ИС; A_i – событие, состоящее в нарушении безопасности i-го компонента сложной ИС в результате атаки.

Расчеты по формуле (1) показывают, что вероятности успешных атак при увеличении сложности ИС составляют:

Для сложности ИС от 1 до10 рабочих мест – до 0,5.

Для сложности ИС до 100 рабочих мест – 0,7.

Для сложности ИС до 1000 рабочих мест – 0,85.

Таким образом, для сложных систем ИС и АС необходимы дополнительные меры по обеспечению безопасности и защиты информации именно сложных систем.

В связи с этим, во-первых, предлагается ввести дополнительную классификацию ИС по уровню их сложности:

- класс 1 для сложности ИС выше 1000 рабочих мест;
- класс 2 для сложности ИС от 100 до 1000 рабочих мест;
- класс 3 для сложности ИС от 10 до 100 рабочих мест;
- класс 4 для сложности ИС до 10 рабочих мест.

Во-вторых, в соответствии с дополнительной классификацией требований необходимых мер по компенсации угроз безопасности современных ИС ФСТЭК России (без учета роста их сложности) предлагается ввести их классификацию по уровню сложности ИС.

Эти дополнительные требования и меры для сложных ИС дополняют перечень мер, изложенных в перечне мер и требований ФСТЭК России и ГОСТ Р.

Предлагаемые существующими нормативными документами меры реализации требований сгруппированы нами в пять категорий.

Категория 1 – традиционная категория мер защиты, в которой существо необходимых мер не зависит от уровня сложности ИС и АС. От уровня сложности систем зависят количественные параметры числа субъектов и защищаемых объектов.

Категория 2 – является основной в определении необходимых и достаточных для номенклатуры и содержания мер защиты и безопасности современных ИС и АС.

Категория 3 – включает меры, ориентированные на программные и технические платформы, к которым могут и должны предъявляться требования и использоваться меры отдельно от требований и мер защиты функционального комплекса.

Категория 4 – относится к важнейшей категории технологий проектирования и создания ИС, совершенно изолированной по составу и содержанию по своим требованиям от требований к функциональным системам.

Категория 5 – в данной статье не обсуждается.

Группы мер защиты информации для реализации требований к ИС, предусмотренные существующими документами ФСТЭК России и ГОСТ Р:

1) идентификация и аутентификация субъектов доступа и объектов доступа;
2) управление доступом субъектов доступа к объектам доступа;
3) ограничение программной среды;
4) защита машинных носителей информации;
5) регистрация событий безопасности;
6) антивирусная защита;
7) обнаружение вторжений;
8) контроль (анализ) защищенности информации;
9) обеспечение целостности;
10) обеспечение доступности;
11) защита среды виртуализации;
12) защита технических средств;
13) защита автоматизированной системы и ее компонентов;
14) обеспечение безопасной разработки программного обеспечения;
15) управление обновлениями программного обеспечения;
16) планирование мероприятий по обеспечению защиты информации;
17) обеспечение действий в нештатных (непредвиденных) ситуациях;
18) информирование и обучение персонала;
19) анализ угроз безопасности информации;
20) выявление инцидентов и реагирование на них и рисков от их реализации.

Однако, перечисленные меры не включают в себя **учет классификации мер сложности ИС.**

В рамках учета уровня сложности ИС предлагается:

- для ИС первого класса сложности должны выполняться все позиции с 1 по 20 с реконструированием и модификацией параметров мер защиты;
- для ИС второго класса сложности должны выполняться нечетные позиции перечня;
- для ИС третьего класса сложности должны выполняться выборочные позиции перечня;
- для четвертого класса сложности ИС предлагается выполнение отдельных позиций перечня.

Для решения вопроса о месте указанных мер с учетом сложности ИС они сгруппированы в категории, связанные с целевой группой требований.

Категория 1. Меры по управлению доступом, регистрацией и учетом, обеспечением целостности:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- обеспечение целостности;
- обеспечение доступности.

Категория 2. События безопасности:

- регистрация событий безопасности;
- антивирусная защита;
- обнаружение вторжений;
- обеспечение действий в нештатных (непредвиденных) ситуациях;
- анализ угроз безопасности информации;
- выявление инцидентов и реагирование на них и рисков от их реализации.

Категория 3. Меры по защите программной и технических платформ, а также функциональных компонент ИС:

- ограничение программной среды;
- защита машинных носителей информации;
- защита среды виртуализации;
- защита технических средств;
- защита автоматизированной системы и ее компонентов;
- управление конфигурацией автоматизированной системы и системы защиты;
- управление обновлениями программного обеспечения.

Категория 4. Меры по защите проектирования и разработки ИС:

- обеспечение безопасной разработки программного обеспечения;
- управление обновлениями программного обеспечения.

Категория 5. Организационные меры:

- планирование мероприятий по обеспечению защиты информации;
- информирование и обучение персонала.

При этом, практически все приведенные группы мер защиты и обеспечения безопасности могут быть реализованы на криптографической платформе.

Заключение

Объективные тенденции роста сложности ИС и АС, рост поля угроз требуют исследований по обеспечению защищенности и безопасности сложных ИС и АС. Необходима более детальная классификация требований по обеспечению информационной безопасности в зависимости от уровня сложности ИС и АС.

Предложенная классификация мер и требований обеспечения информационной безопасности с учетом уровня метрической сложности ИС решает проблему лишь частично.

В дальнейшем необходима разработка регламента модификации требований по безопасности в соответствии с динамикой изменения текущих характеристик ИС и АС, уровня их структурной и функциональной сложности, а также характеристик поля угроз.

Для обоснования новых требований и мер безопасности необходима разработка новых методов и средств адекватного противодействия растущему полю угроз, которые на текущем этапе должны включать следующие компоненты:

- учет и использование методов учета динамики роста сложности функциональных систем;
- систему текущего мониторинга поля угроз безопасности;
- коллективную систему накопления и анализа динамики поля угроз с созданием и организацией обмена информацией между взаимодействующими функциональными системами по текущим видам и номенклатуре угроз безопасности;
- аналитическую систему прогнозирования динамики поля угроз и разработки опережающих мер защиты и безопасности.

Литература

1. РД АС – Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. – М.: ФСТЭК России, 1992.

2. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Руководящий документ. Утверждено приказом ФСТЭК России от 14 марта 2014 г. № 31 – М.: ФСТЭК России, 2014.

3. Липаев В. В. Экономика производства сложных программных продуктов. – М.: СИНТЕГ, 2008. – 432 с.

4. Медведовский И. Д. ISO 17799: Эволюция стандарта в период 2002 – 2005 // DailySec.ru [Электронный ресурс]. 27.12.2007. – URL: http://daily.sec.ru/2005/12/27/I-Medvedovskiy-ISO-17799-evolutsiya-standarta-v-period-2002---2005.html (дата обращения 25.12.2016).

5. Стандарт ISO/IEC 27006:2007. Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью. – М.: Стандартинформ, 2010. – URL: http://files.stroyinf.ru/data2/1/4293820/4293820744.htm (дата обращения 25.12.2016).

6. ISO/IEC FDIS 17799:2005. Information technology – Security techniques.- Code of practice for information security management. – ITTF, 2005. 129 p. – URL: http://comsec.spb.ru/matherials/is/iso17799-2005.pdf (дата обращения 25.12.2016).

7. ISO/IEC FDIS 27001:2005. Information technology - Security techniques - Information security management systems – Requirements. ISO/IEC, 2005. 42 p. – URL: https://infosecprimer.files.wordpress.com/2013/06/iso_iec_27001.pdf (дата обращения 25.12.2016).

8. Нестерук Г. Ф., Осовецкий Л. Г., Нестерук Р. Ш. К разработке модели адаптивной защиты информации // Специальная техника. 2005. № 2. С. 52-58.

References

1. *Avtomatizirovannye sistemy. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiia avtomatizirovannykh sistem i trebovaniia po zashchite informatsii. Rukovodiashchii dokument* [Automated systems. Protection against unauthorized access to information. Automated systems classification and requirements for protection of information. Guidance document]. Approved by the decision of the Chairman of the State technical Commission under the President of the Russian Federation dated 30 March 1992. Moscow, FSTEC of Russian, 1992. (in Russian).

2. *Ob utverzhdenii trebovanii k obespecheniiu zashchity informatsii v avtomatizirovannykh sistemakh upravleniia proizvodstvennymi i tekhnologicheskimi protsessami na kriticheski vazhnykh ob"ektakh, potentsial'no opasnykh ob"ektakh, a takzhe ob"ektakh, predstavliaiushchikh povyshennuiu opasnost' dlia zhizni i zdorov'ia liudei i dlia okruzhaiushchei prirodnoi sredy* [On approval of requirements for ensuring information protection in automated control systems of production and technological processes at critically important objects, potentially hazardous objects and objects of increased danger to life and health of people and the natural environment]. Approved by order FSTEK of Russia from March 14, 2014 No. 31. Moscow, FSTEC of Russia, 2014. (in Russian).

3. Lipaev V. V. *Ekonomika proizvodstva slozhnykh programmnykh produktov* [Economics of production of complex software products]. Moscow, SINTEG Publ., 2008. 432 p. (in Russian).

4. Medvedovskii I. D. ISO 17799: Evoliutsiia standarta v period 2002 – 2005 [ISO 17799: the evolution of the standard in the period 2002 – 2005]. DailySec.ru, 27 December 2007. Available at: http://daily.sec.ru/2005/12/27/I-Medvedovskiy-ISO-17799-evolutsiya-standarta-v-period-2002---2005.html (in Russian) (accessed 25 December 2016).

5. Standard ISO/IEC 27006:2007. Information technology. Security techniques. Requirements for auditing bodies and certification of information security management systems. 2007. 44 p. Available at: http://www.pqm-online.com/assets/files/lib/std/iso_iec_27006-2007.pdf (accessed 25 December 2016).

6. ISO/IEC FDIS 17799:2005. Information technology – Security techniques.- Code of practice for information security management. ITTF, 2005. 129 p. – Available at: http://comsec.spb.ru/matherials/is/iso17799-2005.pdf (accessed 25.12.2016).

7. ISO/IEC FDIS 27001:2005. Information technology - Security techniques - Information security management systems – Requirements. ISO/IEC, 2005. 42 p. – Available at: https://infosecprimer.files.wordpress.com/2013/06/iso_iec_27001.pdf (accessed 25.12.2016).

8. Nesteruk G. F., Osovetskiy L.G., Nesteruk R. Sh. To develop a model of adaptive information protection. Special equipment, 2005, no. 2, pp. 52-58.

Статья поступила 26 декабря 2016 г.

Сведения об авторах

Осовецкий Леонид Георгиевич – доктор технических наук, профессор, лауреат государственной премии совета министров СССР. Советник генерального директора. Ленинградское отделение Центрального научно-исследовательского института связи (ЛО ЦНИИС). Область научных интересов: информационная безопасность, безопасность программных средств. E–mail: leoned.osovetsky@gmail.com

Суханов Андрей Вячеславович – доктор технических наук. Заместитель директора по науке. ООО «Эврика». Область научных интересов: информационная безопасность. E–mail: avsuhanov@eureca.ru

Ефимов Вячеслав Викторович – кандидат технических наук, доцент. Директор института. Ленинградское отделение Центрального научно-исследовательского института связи (ЛО ЦНИИС). Область научных интересов: инновационные решения и перспективы развития транспортных сетей связи. E–mail: vve@loniis.ru

Адрес: Россия, 196128, Санкт-Петербург, ул. Варшавская, 11.

Measures to Ensure Security and Data Protection for Complex Information Systems

L. G. Osovetskiy, A. V. Sukhanov, V. V. Efimov

Problem statement: *the number of elements in information systems is increasing therefore, their complexity increases too. Requirements for information security are required to present, depending on the complexity of the information system. The existing requirements on information security and the means that it does not take into account the complexity of the information system. Requirements on information security should be categorized and modified depending on the classification of the complexity of the information system. For the complex information system, you need to consider the connections between its elements and the system effects of a security breach for the individual elements.* ***The aim of this paper*** *is to analyze how the complexity of information sysytems influence on their information security and protection. In addition, the aim of the paper is the classification of requirements in information security to the information systems by the criterion of "complexity–security" and formulation the methods that take into account the complexity of the information system. This will allow you to build a security subsystem and data protection, which is adequate to the threats and level of complexity of the information system.* ***Methods used.*** *The paper uses methods of system analysis for complex systems and classification methods, which are used for the analysis of information security of information systems.* ***Result.*** *Requirements for information security and means their to ensure that classified the level of complexity of the protected system presented in the paper. The paper shows that these requirements can be simplified for the simple information systems need to improve for the complex systems. The number of elements and their connections must be considered when increasing demands for the complex systems.* ***Novelty.*** *A new result is that, given the complexity of the system while the formation of the requirements to information security and means of providing it.* ***Practical significance.*** *The results of this paper can be used for the establishment of regulatory requirements for information security of complex information systems, for certification of complex information objects, for design of security systems for complex information systems.*

Keywords*: information system, security, information security, security threats and protection measures, regulatory requirements.*

Information about Authors

Leonid Georgievich Osovetskiy – Dr. habil. of Engineering Sciences, Professor, Advisor of CEO. Leningrad Branch of Central Science Research Telecommunication Institute (LO ZNIIS). Field of research: information security, security software. E–mail: leoned.osovetsky@gmail.com

Andrei Viacheslavovich Sukhanov – Dr. habil. of Engineering Sciences. Deputy Director for science. Evrika ltd. Field of research: information security. E–mail: avsuhanov@eureca.ru

Vyacheslav Viktorovich Efimov – Ph.D. of Engineering Sciences, Associate Professor. CEO of Institute. Leningrad Branch of Central Science Research Telecommunication Institute (LO ZNIIS). Field of research: innovations in telecommunications. E–mail: vve@loniis.ru

Address: Russia, 196128, Saint Petersburg, Varshavskaya str., 11.