ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056.57
DOI: 10.21822/2073-6185-2022-49-4-52-57 Оригинальная статья /Original Paper

Расчет коэффициента уровня защищенности автоматизированной системы органов внутренних дел на основе информационной обеспеченности СЗИ обновлениями сигнатур вирусов и угроз

А.О. Ефимов, И.Г. Дровникова, Е.А. Рогозин, В.Р. Романова, Е.В. Филь
Воронежский институт МВД России,
394065, г. Воронеж, пр. Патриотов, 53, Россия

Резюме. Цель. В данной работе рассмотрена защита от угроз, наступающих в большей частоте случаев в период от начала загрузки операционной системы. Рассмотрение различных конфигураций позволит произвести обзор достаточно широкого спектра возникающих ситуаций. Для решения поставленной задачи необходимо осуществить определение уязвимых мест, а также произвести обозначение коэффициентов, определяющих состояние автоматизированной системы. **Метод.** Средствами вычислительной техники являются совокупность программных и технических компонентов (в том числе средств защиты информации) систем обработки данных, способных функционировать самостоятельно или в составе других систем. Применены методы анализа процесса воздействия компьютерных угроз на этапе загрузки операционной системы. **Результат.** Предложена методика расчет коэффициента защищенности автоматизированных систем в защищенном исполнении в зависимости от наличия необходимых политик безопасности и своевременного обновления баз сигнатур вирусов и угроз. Обобщены уязвимости в процессе запуска операционной системы, сделаны выводы о расчете коэффициента уровня защищенности автоматизированной системы ОВД на основе информационной обеспеченности СЗИ обновлениями сигнатур вирусов и угроз. **Вывод.** Разработанная методика позволяет производить оценку защищенности автоматизированных систем с учетом обстановки информационной обеспеченности на местах.

Ключевые слова: оценка защищенности, автоматизированная система, защита информации, средство защиты информации, угроза информации

Для цитирования: А.О. Ефимов, И.Г. Дровникова, Е.А. Рогозин, В.Р. Романова, Е.В. Филь. Расчет коэффициента уровня защищенности автоматизированной системы органов внутренних дел на основе информационной обеспеченности СЗИ обновлениями сигнатур вирусов и угроз. Вестник Дагестанского государственного технического университета. Технические науки. 2022; 49(4):52-57. DOI:10.21822/2073-6185-2022-49-4-52-57

Calculation of the security level coefficient of the automated system of the internal affairs bodies based on the information security of the information security system with updates of virus and threat signatures

A.O. Efimov, I.G. Drovnikova, E.A. Rogozin, V.R. Romanova, E.V. Phil
Voronezh Institute of the Ministry of Internal Affairs of Russia,
53 Patriotov Str., Voronezh 394065, Russia

Abstract. Objective. This paper considers protection against threats that occur more often in the period from the start of the operating system boot. Consideration of various configurations will allow an overview of a fairly wide range of situations that arise. To solve the problem, it is necessary to determine the vulnerabilities, as well as to designate the coefficients that determine the state of the automated system. **Method.** Computer facilities are a set of software and hardware components (including information security tools) of data processing systems that can function independently or as part of other systems. Methods for analyzing the process of the impact of computer threats at the stage of

loading the operating system are applied. **Result.** A technique is proposed for calculating the security factor of automated systems in a secure design, depending on the availability of the necessary security policies and the timely updating of virus and threat signature databases. The vulnerabilities in the process of starting the operating system are summarized, conclusions are drawn on the calculation of the security level coefficient of the automated ATS system based on the information security of the information security system with updates of virus and threat signatures. **Conclusion.** The developed methodology makes it possible to assess the security of automated systems, taking into account the situation of information security in the field.

Keywords: security assessment, automated system, information security, information security tool, information threat

For citation: A.O. Efimov, I.G. Drovnikova, E.A. Rogozin, V.R. Romanova, E.V. Phil. Calculation of the security level coefficient of the automated system of the internal affairs bodies based on the information security of the information security system with updates of virus and threat signatures. Herald of the Daghestan State Technical University. Technical Science. 2022; 49 (4): 52-57. DOI: 10.21822 /2073-6185-2022-49-4-52-57

Введение. В данный момент крайне актуальными являются вопросы защищенности автоматизированных систем от компьютерных и иных преднамеренных угроз. Определенно существует огромное множество угроз. В данной работе будет рассмотрена защита от угроз, наступающих в периоде от начала загрузки операционной системы.

Рассмотрение различных конфигураций позволит произвести обзор достаточно широкого спектра возникающих ситуаций. В данной предметной области средствами вычислительной техники являются совокупность программных и технических компонентов (в том числе средств защиты информации) систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Постановка задачи. В целях расчета коэффициента уровня защищенности автоматизированной информационной системы, необходимо произвести анализ процесса воздействия компьютерных угроз на этапе загрузки операционной системы. Для решения поставленной задачи, необходимо осуществить определение уязвимых мест, а также произвести обозначение коэффициентов, определяющих то либо иное состояние автоматизированной системы.

Методы исследования. В первую очередь рассмотрим порядок загрузки семейства операционных систем Windows и Linux-подобных операционных систем (рис.1).

Рис.1. Схема порядка запуска операционной системы
Fig.1. Scheme of the order of starting the operating system

Порядок загрузки операционных систем Windows и Linux довольно схож, процедуры, протекающие в процессе запуска, выполняют одни и те же функции.

На первых пяти этапах запуска, происходят выполнение команд загрузки, зависящих от настроек BIOS, и носителей данных. На этих этапах рекомендуется применять средства защиты информации от несанкционированного доступа с функционалом доверенной загрузки [1].

Одним из наиболее узких мест является передача управления от загрузчика верхнего уровня к загрузчику операционной системы. Конечно, современные средства защиты информации разработаны таким образом, что своевременно противодействуют возникающим угрозам и перекрывают множество уязвимых мест [2]. Но обеспеченность защиты средствами защиты напрямую зависит от качества информационной обеспеченности средств защиты информации, а также всей остальной системы в целом. В последнее время все чаще стали обнаруживаться уязвимости, связанные с ошибками в проектировании ряда центральных процессоров, а также уязвимостей связанных с применением различных наборов инструкций и взаимодействия вместе с ними операционной системы [4].

Основой рассматриваемых угроз являются: УБИ.214 (угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации), УБИ.217 (угроза использования скомпрометированного доверенного источника обновлений программного обеспечения), УБИ.192 (угроза использования уязвимых версий программного обеспечения) [5].

В условиях наличия неопределенного числа уязвимостей жизненно необходимо иметь постоянное обновление средств защиты информации, антивирусов, файрволла, а также полного набора патчей безопасности операционной системы.

Но и даже в этом случае все не так однозначно: системы, применяемые вне локальных сетей и сети Интернет, обрабатывающие лишь локальную информацию, по своей сути не требуют дополнительной оценки защищенности в связи с отсутствием каналов получения программных угроз. Поэтому предлагается рассмотреть ряд различных конфигураций АРМ, и привести ряд ситуаций к общему коэффициенту.

Определим основные параметры, которые будут иметь значение при расчёте коэффициента (буквенные обозначения определены в скобках):

1. Наличие подключенного к АРМ сетевого соединения (A);
2. Наличие средств защиты информации от несанкционированного доступа (B);
3. Определен ли ряд носителей, с помощью которых возможно вносить информацию на АРМ (C);
4. Наличие средств антивирусной защиты (D);
5. Наличие программного или программно-аппаратного межсетевого экрана (E);
6. Своевременность обновления баз данных сигнатур вирусов и угроз (коэффициент информационной обеспеченности) (X);
7. Число элементов, участвующих в расчете (Z).

В качестве показателей, характеризующих процесс оценки защищенности АС ОВД, предлагается выбрать вероятности преодоления злоумышленником средства защиты, из совокупности которых будет складываться оценка защищенности.

$$P_{защ} = 1 - \prod_{m=1}^{k} P_{преод_m} \quad (1)$$

где k – количество средств защиты, которые необходимо преодолеть злоумышленнику, чтобы получить доступ к ресурсам;

P – вероятность преодоления нарушителем m-ого средства защиты.

Определим общий коэффициент уровня защищенности АС ОВД на основе информационной обеспеченности СЗИ. Для решения выше поставленной цели определим составные части:

1. Параметры 1, 2, 4, 5 будут влиять, на величину непосредственно и принимать значения 0, 1. Это будет указывать на наличие того, либо иного элемента в системе: 1 – В системе

присутствует элемент; 0 – Элемент в системе отсутствует (в случае параметра 1 не влияет на уровень угроз, в остальных случаях снижает защиту).

2. Параметр 3 будет учитывать, определены ли носители информации с помощью, которых будет вноситься информация в АС. Будет принимать следующие значения: 1 – Носители определены и используются исключительно среди защищенных и контролируемых АС; 0.5 – Носители определены; 0 – Носители не определены, в систему вносится информация с неопределенного числа носителей (повышает риски безопасности).

3. Параметр 7 напрямую зависит от параметра 1, если A = 1, то Z=4, иначе Z=4.

4. Параметр 6 определяет информационную обеспеченность средств защиты информации, и указывает насколько средства защиты получают обновления:

- все обновления средств защиты поступают автоматически и незамедлительно X=1;
- обновления СЗИ поступают незамедлительно лишь до части средств, остальные в ручном режиме X=0.8;
- обновления средств защиты информации поступают в скорые сроки в ручном режиме X=0.6;
- обновления поступают несвоевременно в ручном режиме X=0.4;
- обновления антивирусной системы и межсетевого экрана производятся, иные средства ЗИ не обновляются X=0.2;
- обновления не производятся X=0.

Соотнесем полученную информацию и составим итоговую формулу коэффициента уровня защищенности автоматизированной системы ОВД на основе информационной обеспеченности СЗИ обновлениями сигнатур вирусов и угроз:

$$K = \frac{(A*B)+C+D+E}{Z} * X \quad (2)$$

где A – наличие подключенного к АРМ сетевого соединения;

B – наличие средств защиты информации от несанкционированного доступа;

C – определен ли ряд носителей с помощью, которых возможно вносить информацию на АРМ;

D – наличие средств антивирусной защиты;

E – наличие программного или программно-аппаратного межсетевого экрана;

Z – число элементов, участвующих в расчете;

X – своевременность обновления баз данных сигнатур вирусов и угроз (коэффициент информационной обеспеченности).

Данный коэффициент подставим в формулу (1), и получим формулу, осуществляющую расчет защищенности в зависимости от вероятности преодоления злоумышленником средства защиты с учетом зависимостей от информационной обеспеченности.

$$P_{\text{защ.ИО}} = \left(1 - \prod_{m=1}^{k} P_{\text{преод.}}\right) * K \quad (3)$$

Данная формула должна позволить производить расчет защищенности схожих по своей конструкции систем, но с учетом конкретных особенностей настройки и установки системы. Стоит обратить внимание, что при наличии полного набора средств защиты, и их своевременном обновлении, риски значительно снижаются.

Обсуждение результатов. В качестве вычислительного эксперимента произведем корректировку величины защищенности схожих по своей структуре АС (табл.1).

За основу возьмем начальную величину защищенности равную 0.8.

Таблица 1. Задаваемые параметры
Table 1. Parameters to be set

№ АС	A	B	C	D	E	Z
1.	1	1	0.5	0	0	4
2.	0	1	0.5	1	1	3

Из полученных данных получим следующее распределение защищенности:

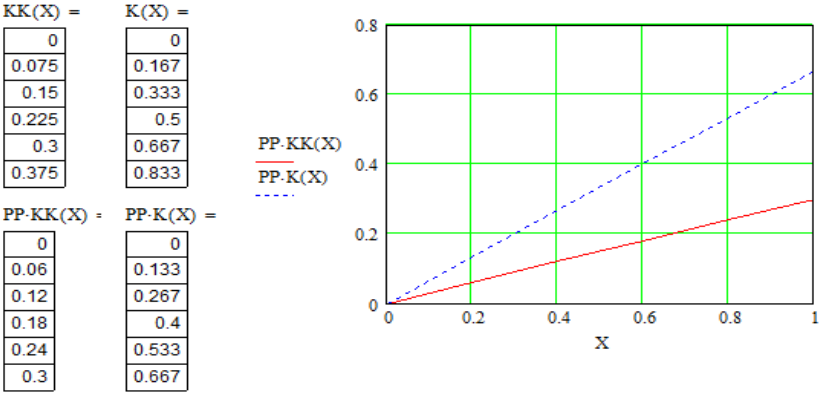

Рис. 2. Реализация расчета в системе Mathcad
Fig. 2. Implementation of the calculation in the Mathcad system

Как видно на рис.2, наличие антивирусной системы и средств ЗИ от несанкционированного доступа позволили значительно сохранить уровень защищенности, рассчитанный с учетом коэффициента информационной обеспеченности. Чего нельзя сказать про другой случай, когда влияние этого коэффициента оказалось слишком велико и привело к потерям почти более чем в 2 раза.

Вывод. В работе произведено рассмотрение вопросов расчета коэффициента защищенности автоматизированных систем в защищенном исполнении в зависимости от наличия необходимых политик безопасности и своевременного обновления баз сигнатур вирусов и угроз.

Обобщены уязвимости в процессе запуска операционной системы, сделаны выводы о расчете коэффициента уровня защищенности автоматизированной системы ОВД на основе информационной обеспеченности СЗИ обновлениями сигнатур вирусов и угроз.

Разработанная методика может позволить производить оценку защищенности автоматизированных систем с учетом обстановки информационной обеспеченности на местах.

Библиографический список:

1. Об утверждении Наставления по технической эксплуатации средств связи и автоматизации территориальных органов Министерства внутренних дел Российской Федерации: приказ МВД России от 30.11.2016 № 772 // Информационно-правовой портал системы КонсультантПлюс. – Режим доступа: http://base.consultant.ru (дата обращения: 15.02.2022).
2. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России от 18.02.2013 № 21 // Информационно-правовой портал системы КонсультантПлюс. – Режим доступа: http://base.consultant.ru (дата обращения: 27.02.2022).
3. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11.02.2013 № 17 // Информационно-правовой портал системы КонсультантПлюс. – Режим доступа: http://base.consultant.ru (дата обращения: 15.02.2022).
4. Методика оценки угроз безопасности информации: Методический документ ФСТЭК России от 05.02.2021 // Информационно-правовой портал системы КонсультантПлюс. – Режим доступа: http://base.consultant.ru (дата обращения: 27.10.2022).
5. Банк данных угроз безопасности информации: [Электронный ресурс]. ФСТЭК России. URL: https://bdu.fstec.ru/. (Дата обращения: 27.10.2022).
6. ФСТЭК РФ. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения.
7. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения //М.: Федеральное агентство по техническому регулированию и метрологии. 2006. 12 с.
8. ГОСТ Р 56546–2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. 2016. 8с.
9. ФСТЭК РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
10. ГОСТ Р 15408–2013. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий // М.: Стандартинформ. 2014. 152 с.
11. ГОСТ Р 53114–2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. 2008. 22с.
12. Руководящий документ. Безопасность информационных технологий. Концепция оценки соответствия автоматизированных систем требованиям безопасности информации: утв. ФСТЭК России 2004 г.

13. Руководящий документ Гостехкомиссии. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий: утв. Приказом Гостехкомиссии от 19.06.2002 №187.
14. Методика определения угроз безопасности информации в информационных системах: утв. ФСТЭК России 2015 г.
15. Коцыняк М.А., Кулешов И.А., Кудрявцев А.М., Лаута О.С. Киберустойчивость ИТКС. СПб, 2015 г.

References:

1. On the approval of the Manual on the technical operation of communications and automation of the territorial bodies of the Ministry of Internal Affairs of the Russian Federation: order of the Ministry of Internal Affairs of Russia dated November 30, 2016;772. *Information and legal portal of the ConsultantPlus syste*m. – Access mode: http://base.consultant.ru (date of access: 15.02.2022). (In Russ)
2. On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems: order of the FSTEC of Russia dated February 18, 2013; 21. *Information and legal portal of the ConsultantPlus system*. – Access mode: http://base.consultant.ru (date of access: 02/27/2022). (In Russ)
3. On approval of the Requirements for the protection of information that is not a state secret contained in state information systems: order of the FSTEC of Russia dated February 11, 2013; 17. *Information and legal portal of the ConsultantPlus system.* – Access mode: http://base.consultant.ru (date of access: 02/15/2022). (In Russ)
4. Methodology for assessing threats to information security: Methodological document of the FSTEC of Russia dated 02/05/2021 // *Information and legal portal of the ConsultantPlus system*. – Access mode: http://base.consultant.ru (date of access: 10/27/2022).FSTEC of the Russian Federation. Guidance document. Protection against unauthorized access to information. Terms and definitions. (In Russ)
5. Data bank of information security threats: [Electronic resource]. FSTEC of Russia. URL: https://bdu.fstec.ru/. (Date of access: 27.10.2022). (In Russ)
6. FSTEC RF. Management document. Protection against unauthorized access to information. Terms and Definitions.
7. GOST R 50922-2006. Information protection. Basic terms and definition // Moscow: Federal Agency for Technical Regulation and Metrology. 2006.12 K. (In Russ)
8. GOST R 56546-2015. Information protection. Communications of information systems. Classification of information systems. 2016; 8. (In Russ)
9. FSTEC of the Russian Federation. Guidance document. Automated systems. Protection against unauthorized access to information. Classification of automated systems and information security requirements. (In Russ)
10. GOST R 15408-2013. Methods and means of ensuring security. Criteria for assessing the security of information technologies / / Moscow: Standartinform. 2014;152. (In Russ)
11. GOST R 53114-2008. Information protection. Ensuring information security in the organization. Basic terms and definitions. 2008; 22. (In Russ)
12. Guidance document. Information technology security. The concept of assessing the compliance of automated systems with information security requirements: approved by FSTEC of Russia 2004. (In Russ)
13. The guiding document of the State Technical Commission. Information technology security. Criteria for assessing the security of information technologies: approved. By Order of the State Technical Commission No. 187 dated 06/19/2002. (In Russ)
14. Methodology for determining the risk of information security in information systems: approved by FSTEC of Russia 2015. (In Russ)
15. Kotsynyak M. A., Kuleshov I. A., Kudryavtsev A.M., Lauta O. S. Cyberstability of ITCS. St. Petersburg, 2015. (In Russ)

Сведения об авторах:

Ефимов Алексей Олегович, адъюнкт очной формы обучения; ea.aleksei@yandex.ru

Дровникова Ирина Григорьевна, доктор технических наук, доцент, профессор кафедры автоматизированных информационных систем органов внутренних дел; idrovnikova@mail.ru

Рогозин Евгений Алексеевич, доктор технических наук, профессор, профессор кафедры автоматизированных информационных систем органов внутренних дел; evgenirogozin@yandex.ru

Романова Виктория Романовна, адъюнкт очной формы обучения; romanovna_vika@inbox.ru

Филь Елизавета Вадимовна, курсант 4 курса радиотехнического факультета; fillichkina@yandex.ru

Information about authors:

Aleksey O. Yefimov, full-time adjunct; ea.aleksei@yandex.ru

Irina G. Drovnikova, Dr. Sci. (Eng.), Prof., Assoc. Professor, Department of Automated Information Systems of Internal Affairs Bodies; idrovnikova@mail.ru

Evgeny A. Rogozin, Dr. Sci. (Eng.), Prof., Prof., Department of Automated Information Systems of Internal Affairs Bodies; evgenirogozin@yandex.ru

Victoria R. Romanova, adjunct of full-time education; romanovna_vika@inbox.ru

Elizaveta V. Fil, 4th year cadet of the Faculty of Radio Engineering; fillichkina@yandex.ru

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 29.10.2022.

Одобрена после рецензирования/ Reviced 18.11.2022.

Принята в печать/Accepted for publication 18.11.2022.