ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI:10.21822/2073-6185-2023-50-4-101-108

Оригинальная статья/ Original article

Об отдельных аспектах стандартизации и условий функционирования автоматизированных систем

А.О. Ефимов[1], И.И. Лившиц[2], М.О. Мещеряков[3], Е.А. Рогозин[4], В.Р. Романова[5]
[1,4,5] Воронежский институт МВД России,
[1,4,5] 394065, г. Воронеж, пр. Патриотов, 53, Россия,
[2] Национальный исследовательский университет ИТМО,
[2]197101,г.Санкт-Петербург, Кронверкский пр., д. 49, Россия,
[3] Московский государственный технический университет имени Н.Э. Баумана,
[3]105005, г. Москва, 2-я Бауманская улица, 5, стр. 1, Россия

Резюме. Цель. Рассмотрены основные аспекты условий функционирования АС, а также вопросы стандартизации стадий жизненного цикла АС (создания, ввода в эксплуатацию, сопровождения и пр.) на государственном уровне. В данной предметной области рассматриваются технологические особенности построения АС на базе различных технических архитектур, так как в настоящее время применимы как зарубежные процессоры на базе архитектур x86-64, так и процессоры отечественной разработки на основе архитектуры ARM (Advanced RISC Machine). Применение различных компонент АС требует дополнительной проработки вопросов с точки зрения упорядочивания состава и конфигурации конкретных СЗИ. Многоуровневая архитектура процессора объективно усложняет возможности для полного тестирования безопасности и обнаружения всех уязвимостей. **Метод.** Аналитически обобщена информация об основных государственных стандартах, применяемых для обеспечения защиты информации в АС в настоящее время. **Результат.** Рассмотрены основные особенности условий функционирования АС и определено, что уязвимости компонент обусловлены несовершенством процедур разработки и покрытия тестирования технических и программных средств. Определено, что для осуществления защиты информации в АС необходимо построение многоуровневой системы защиты с государственной аккредитацией. **Вывод.** Представлены предложения для области применения государственной стандартизации для защиты информации в АС с учетом текущего и перспективного ландшафта угроз, в том числе с учетом конструктивных особенностей (недекларированных возможностей) компонент. Преодоление угроз возможно при создании многоуровневой системы защиты информации с государственной аккредитацией.

Ключевые слова: автоматизированная система, защита информации, средство защиты информации, угроза, уязвимость

Для цитирования: А.О. Ефимов, И.И. Лившиц, М.О. Мещеряков, Е.А. Рогозин, В.Р. Романова. Об отдельных аспектах стандартизации и условий функционирования автоматизированных систем. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(4):101-108. DOI:10.21822/2073-6185-2023-50-4-101-108

On certain aspects of standardization and operating conditions of automated systems

A.O. Efimov[1], I.I. Livshits[2], M.O. Meshcheryakov[3], E.A. Rogozin[4], V.R. Romanova[5]
[1,4,5]Voronezh Institute of the Ministry of Internal Affairs of Russia,
[1,4,5]53 Patriotov Ave., Voronezh 394065, Russia,
[2] N.E. Bauman Moscow State Technical University,
[2] 2nd Baumanskaya St. 5, p.1, Moscow 105005, Russia,
[3] National Research University ITMO,
[3]49 Kronverksky Ave., St. Petersburg 197101, Russia

Abstract. **Objective**. In this paper, the main aspects of the operating conditions of the AS are considered, as well as the issues of standardization of the stages of the life cycle of the AS (creation, commissioning, maintenance, etc.) at the state level. In this subject area, the technological features of building an AS based on various technical architectures are briefly considered, since both foreign processors based on x86-64 architectures and processors of domestic development based on the Advanced RISC Machine architecture are currently applicable. The use of various components of the AS requires additional study in terms of ordering the composition and configuration of specific SPI. Since each processor has a multi-level architecture, this fact objectively complicates the possibilities for full security testing and detection of all vulnerabilities. **Method**. In the course of the work, the threats and vulnerabilities of individual components of the AS from the point of view of intentional and unintentional threats are considered. The information on the main state standards applied to ensure the protection of information in the AS at the present time is summarized. **Result**. The main features of the operating conditions of the AS are considered and it is determined that the vulnerabilities of the components are due to the imperfection of the procedures for developing and covering testing of hardware and software. It is determined that in order to protect information in the AS, it is necessary to build a multi-level protection system with state accreditation. **Conclusion**. Proposals are presented for the application of state standardization for the protection of information in the AS, taking into account the current and prospective threat landscape, including taking into account the design features (undeclared capabilities) of the components. Overcoming threats is possible with the creation of a multi-level information protection system with state accreditation.

Keywords: automated system, information protection, information security tool, threat, vulnerability

For citation: A.O. Efimov, I.I. Livshits, M.O. Meshcheryakov, E.A. Rogozin, V.R. Romanova. On certain aspects of standardization and operating conditions of automated systems. Herald of Daghestan State Technical University. Technical Sciences. 2023; 50(4):101-108. DOI:10.21822/2073-6185-2023-50-4-101-108

Введение. В настоящее время крайне актуальной является проблема использования в АС информации различной степени конфиденциальности. Для удовлетворения требований различных категорий пользователей разрабатывается значительное количество АС в различных конфигурациях, направленных на эффективное решение конкретного спектра задач в специфических областях [1–3]. Текущие тенденции развития технологий накладывают свой отпечаток на архитектуру и состав компонент в составе конкретных специализированных АС.

Постановка задачи. Постоянное развитие мощности вычислительных (процессорных) компонент, а также объемов хранимой информации и практически неограниченного периметра доступа множества пользователей объективно требует новых методов защиты информации.

Методы исследования. В основе различных технических архитектур в настоящее время применимы как зарубежные процессоры на базе архитектур Intel x86-64, так и процессоры отечественной разработки на основе архитектуры ARM (Advanced RISC Machine). Применение различных типов процессоров, операционных систем (ОС) и СЗИ также требует дополнительной проработки с точки зрения построения современной и адекватной защиты информации под государственным контролем [4 – 9].

Рассмотрим проблемы обеспечения защиты на уровне процессоров. Поскольку каждый конкретный тип процессора обладает многоуровневой архитектурой, это значительно усложняет возможности для полного тестирования функций безопасности и своевременного обнаружения уязвимостей [10,11]. В банке данных угроз безопасности информации (УБИ) ФСТЭК России представлены две УБИ, касающиеся процессоров.

Например, УБИ.209: «Угроза несанкционированного доступа к защищаемой памяти ядра процессора». Угроза заключается в возможности получения доступа к защищенной памяти из программы, не обладающей соответствующими правами, в

результате эксплуатации уязвимостей, позволяющих преодолеть механизм разграничения доступа, реализуемый центральным процессором. Реализация данной УБИ обусловлена наличием уязвимостей, связанных с ошибкой контроля доступа к памяти, основанных на спекулятивном выполнении инструкций процессора. Ошибка контроля доступа обусловлена следующими факторами: отсутствие проверки прав доступа процесса к читаемым областям при спекулятивном выполнении операций, в том числе при чтении из оперативной памяти; отсутствие очистки кэша от результатов ошибочного спекулятивного исполнения; хранение данных ядра операционной системы в адресном пространстве процесса. Реализация данной УБИ возможна из-за наличия процессоров, имеющих аппаратные уязвимости и для которых нет соответствующих обновлений [10]. Отмечается, что данный вид угроз актуален для всех видов и архитектур центрального процессора.

Рассмотрим компонент – оперативная память (Random Access Memory, RAM). В настоящее время применяется RAM 3-го поколения и может быть размещена по-разному: распаяна на плате или подключена как отдельный модуль. Поскольку RAM хранит обрабатываемую информацию различной степени конфиденциальности, она также является уязвимым элементом АС. В банке данных УБИ содержится информация об угрозе УБИ.022: «Угроза избыточного выделения оперативной памяти». Угроза заключается в возможности выделения значительных ресурсов RAM для обслуживания запросов вредоносных программ и соответственного снижения объёма ресурсов RAM, доступной в АС для выделения в ответ на запросы программ легальных пользователей [10]. Данная угроза обусловлена наличием слабостей механизма контроля выделения RAM различным программам. Реализация данной угрозы возможна при условии нахождения вредоносного программного обеспечения в АС в активном состоянии.

Рассмотрим компонент – накопители (жесткие диски, твердотельные накопители (SSD), внешние или мобильные типы накопителей и пр.), которые имеют свои особенности. Поскольку они имеют определенный ресурс, то данный тип компонентов требует своевременного резервного копирования информации, а также точного соблюдения установленных условий эксплуатации. В БДУ ФСТЭК содержится (на дату 16.01.2023) более 44 тыс. уязвимостей. В качестве примера реализации уязвимости рассмотрим BDU:2022-04626: «Уязвимость микропрограммного обеспечения твердотельных накопителей Intel SSD, связанная с одновременным выполнением с использованием общего ресурса с неправильной синхронизацией, позволяющая нарушителю вызвать отказ в обслуживании». В качестве примера УБИ можно привести пример CVE-2022-38392, которая описывает отказ в обслуживании жестких дисков с частотой вращения 5400 об/мин при воздействии злоумышленников, находящихся в непосредственной близости, посредством резонансной частотной атаки считывания файла [12].

Далее рассмотрим компонент – материнскую плату, которая также не является абсолютно безопасным элементом, и по числу возможных уязвимостей ее можно назвать одним из самых уязвимых элементов. Более того, в некоторых случаях уязвимости на типовой материнской плате дополнительно могут возникать при подключении сторонних недоверенных компонентов. Рассмотрим пример угрозы материнской платы – УБИ.004: «Угроза аппаратного сброса пароля BIOS». Реализация данной угрозы основана на аппаратном сбросе пароля, установленного в BIOS/UEFI. Для реализации данной угрозы необходим физический доступ к материнской плате. Отметим, что в БДУ ФСТЭК содержится более 200 уязвимостей, затрагивающих к общем BIOS/UEFI, и 16 УБИ, эксплуатирующих описанные уязвимости конкретных компонентов. Важность рассмотрения различных компонент АС подтверждает тот факт, что каждый конкретный элемент сложной системы может обладать своими уникальными уязвимостями и УБИ, которые эти уязвимости могут эксплуатировать. Среди причин появления уязвимостей можно отметить ошибки проектирования, несовершенство цикла безопасной разработки, а также особенности физического устройства конкретных типов компонент. Вероятно, что некоторые уязвимости могут быть устранены различными способами, самым часто применяемым способом защиты является внедрение программных патчей, либо использование конкретных СЗИ.

В связи с тем, что обнаружение уязвимостей достигается, по большей части, по итогам экспертного анализа уже произошедших успешных атак на конкретные устройства, представляется целесообразным осуществление принципиального контроля защиты от несанкционированного доступа (НСД) к конкретным компонентам в составе АС.

Поскольку физический (непосредственный) и/или удаленный доступ к конкретным компонентам открывает множество уязвимостей, и, соответственно, множество векторов для реализации атак, на практике наблюдается значительное количество СЗИ различного состава и конфигурации. Несмотря на устоявшиеся и хорошо известные архитектурные решения АС, неограниченное множество компонентов аппаратных средств, ОС, встроенных и/или наложенных СЗИ, объективно приводит к известной сложности сопровождения всей совокупности программно-аппаратных компонент в составе АС. Кроме того, необходимо принять во внимание значительные риски применения тех компонент АС, которые находятся в «облаке», вне какого-либо контроля владельца АС или государственных служб, способных контролировать текущий уровень защищенности [13 – 15].

Обсуждение результатов. Система государственных стандартов РФ в области функционирования АС. В качестве нормативно-методической базы в РФ в области функционирования АС применяется ряд государственных стандартов [16,17]. В основе части указанных стандартов находятся зарубежные стандарты (например: ISO, IEC, IEEE или совместные), которые были приняты в национальной системе ГОСТ Р и применяются в РФ в области функционирования АС в РФ. Рассмотрим эволюцию системы государственных стандартов РФ далее на нескольких примерах.

Первый этап предлагается определять в интервале 1995 – 2007 гг., когда были приняты первичные государственные стандарты, регулирующие создание АС в защищенном исполнении (рис. 1). Указанные стандарты определили основы терминологии, основные процедуры проведения испытаний программных средств, общие теоретические сведения, необходимые для построения АС в защищенном исполнении [18,19].

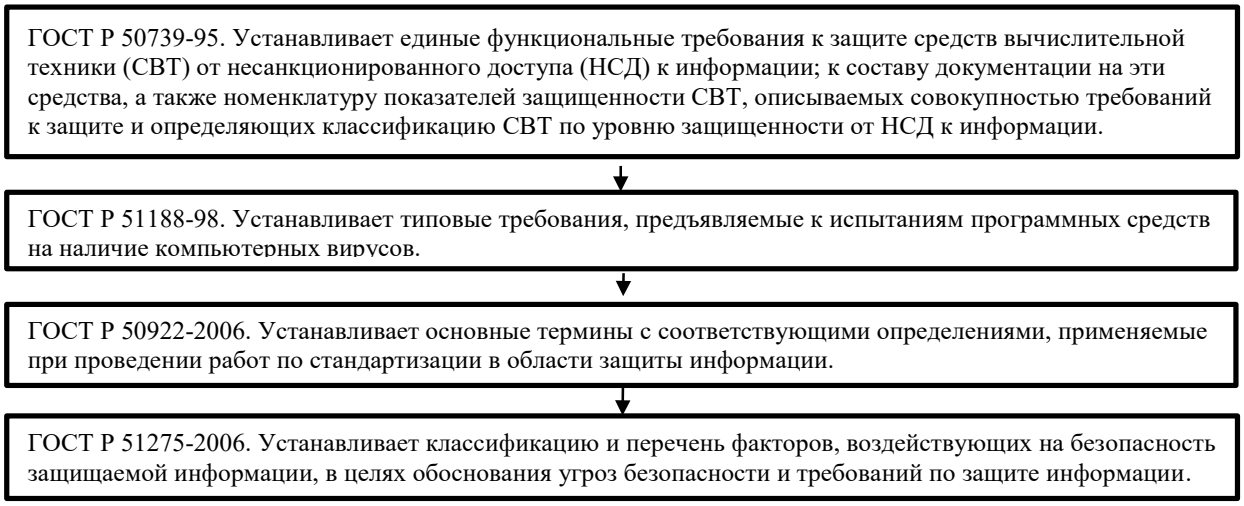

Рис. 1. Схема государственных стандартов, утвержденных в 1995 – 2006 гг.
Fig. 1. Scheme of state standards approved in 1995 – 2006.

Второй этап эволюции системы государственных стандартов предлагается определять в интервале 2007 – 2014 гг., в этот период в РФ продолжается работа по детализации конкретных требований по испытаниям, выявления скрытых каналов, этапов жизненного цикла АС в защищенном исполнении и пр. (рис. 2). В период 2005 – 2021 гг. в РФ активно развивались государственные стандарты, определяющие номенклатуру показателей качества СЗИ, средства контроля эффективности процесса защиты информации, основные термины и определения, связанные с обеспечением защиты информации (рис. 3).

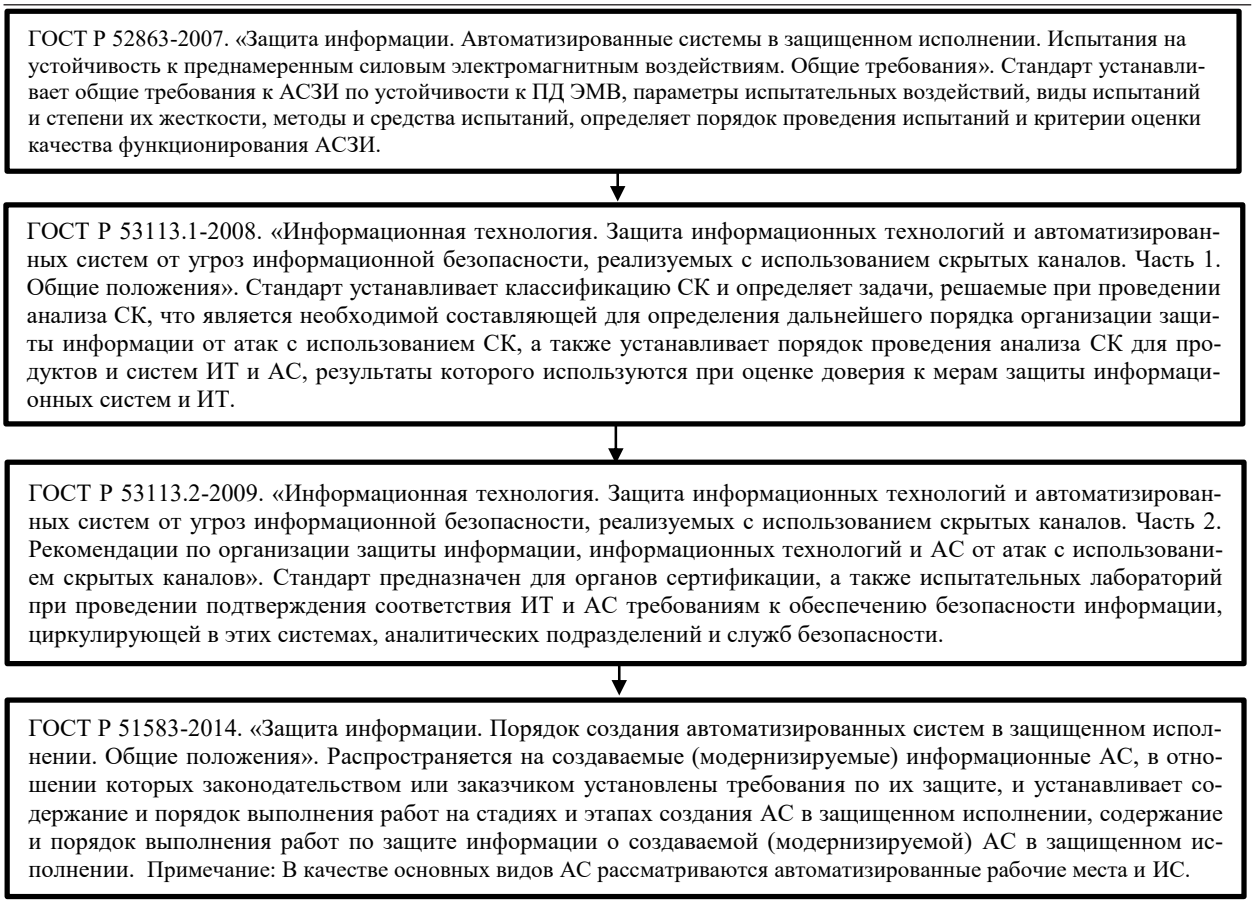

Рис. 2. Схема государственных стандартов, утвержденных в 2007 – 2014 гг.
Fig. 2. Scheme of state standards approved in 2007 – 2014.

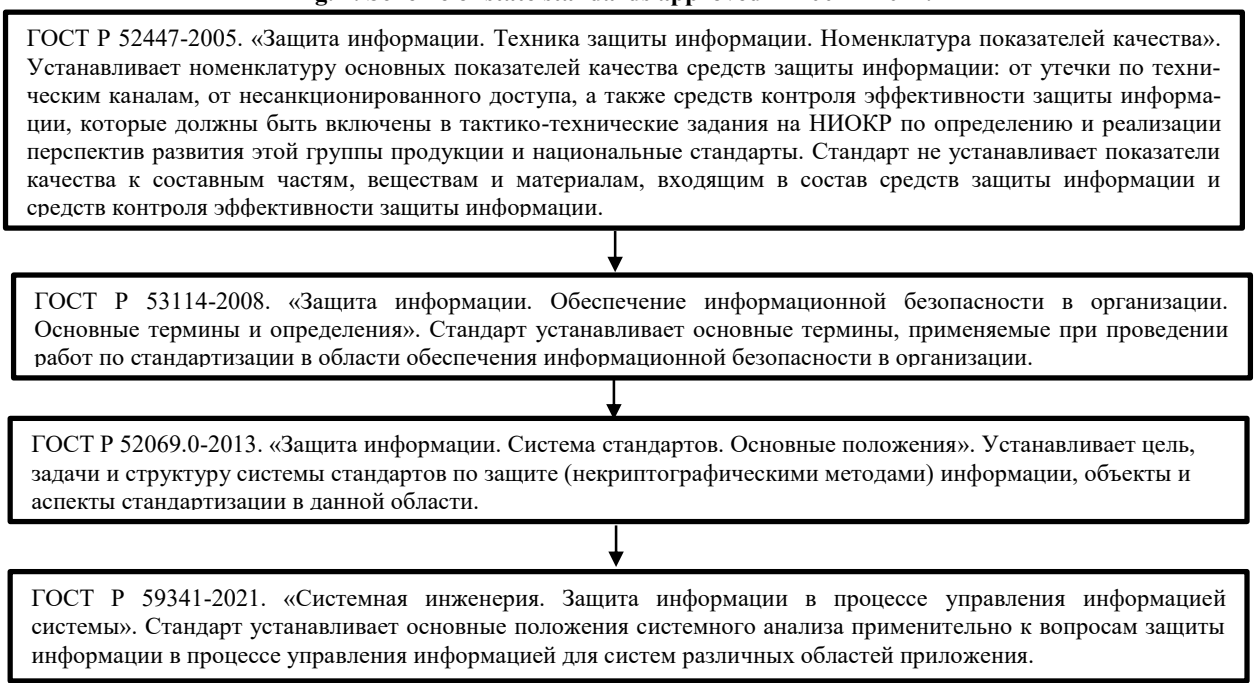

Рис. 3. Стандарты, определяющие основные термины и определения
Fig. 3. Standards defining basic terms and definitions

Отдельное внимание рекомендуется уделять национальным стандартам, которые основаны на международных стандартах ISO, IEC, IEEE и пр. Ценность идентичных стандартов (IDT), корректно переведенных и принятых в системе ГОСТ Р, определяется тем, что существенно экономится время при определении необходимых требований к АС и СЗИ. Наиболее важные стандарты ГОСТ Р ИСО/МЭК показаны на рис. 4.

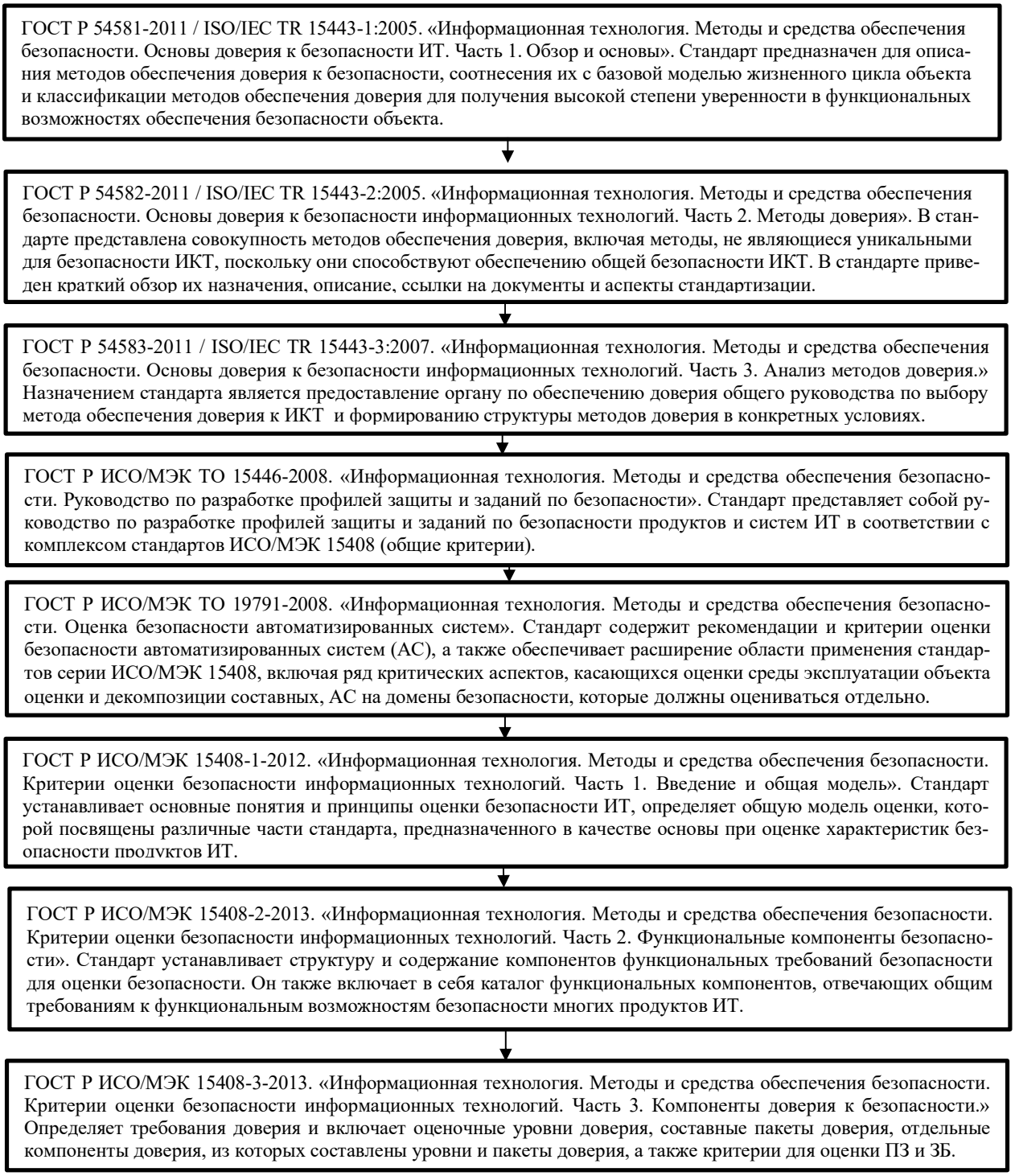

Рис. 4. Стандарты ГОСТ Р ИСО/МЭК, применяемые в сфере защиты информации в АС
Fig. 4. GOST R ISO/IEC standards applied in the field of information security in the AS

Международные стандарты (на 16.01.2023 разработано и опубликовано более 24,5 тыс. только стандартов ISO [20]), позволяют объективно применять лучшую мировую экспертизу в таких областях как управление рисками (ГОСТ Р ИСО/МЭК серии 31000 и 27005), аудитов (ГОСТ Р ИСО серии 19011 и 27006), требованиями к безопасности (ГОСТ Р ИСО/МЭК серии 27001) и пр. (рис. 4).

Вывод. Применительно к области создания АС в защищенном исполнении существует достаточная современная нормативная база стандартизации. Состав базы применимых стандартов определяется как государственными стандартами, разработанными в РФ, так и переводами международных стандартов, принятых в национальной системе ГОСТ Р.

Применение стандарта (совокупности стандартов) определяется спецификой эксплуатации

конкретной АС, составом угроз и множеством уязвимостей, присущих различным компонентам в составе конкретной программно-аппаратной конфигурации. С учетом известных факторов риска необходимо обеспечить в перспективе жизненный цикл АС, основанный на риск-ориентированных стандартах, в том числе – оценку эффективности применения мер защиты, с целью создания национальной эффективной и современной системы обеспечения безопасности.

Библиографический список:

1. Об утверждении Наставления по технической эксплуатации средств связи и автоматизации территориальных органов МВД РФ: приказ МВД России от 30.11.2016 № 772. Информационно-правовой портал системы КонсультантПлюс.Режим доступа: http://base.consultant.ru (16.01.2023).
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: 16.01.2023).
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: 16.01.2023).
4. ФСТЭК России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
5. ГОСТ Р 15408–2013. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. М.: Стандартинформ. 2014. 152 с.
6. ГОСТ Р 53114–2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. 2008. 22с.
7. Руководящий документ. Безопасность информационных технологий. Концепция оценки соответствия автоматизированных систем требованиям безопасности информации:ФСТЭК России, 2004 г.
8. Руководящий документ Гостехкомиссии. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий: утв. пр.м Гостехкомиссии от 19.06.2002 №187.
9. Методика определения угроз безопасности информации в информационных системах: утв. ФСТЭК России. 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: 16.01.2023).
10. Банк данных угроз безопасности информации: [Электронный ресурс]. ФСТЭК России. URL: https://bdu.fstec.ru/. (Дата обращения: 16.01.2023).
11. ФСТЭК России. Руководящий документ. Защита от несанкционированного доступа к информации-Термины и определения. 2015 г.
12. National Vulnerability Database (NVD) CVE-2022-38392: [Электронный ресурс] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38392. (Дата обращения: 16.01.2023)
13. Лившиц И.И. Метод оценивания безопасности облачных ИТ-компонент по критериям существующих стандартов // Труды СПИИРАН. 2020. Т. 19. № 2. С. 383-411.
14. Лившиц И.И., Неклюдов А.В. Суверенные информационные технологии России // Стандарты и качество. 2018. № 4. С. 68-72.
15. Лившиц И.И., Неклюдов А.В. Суверенные информационные технологии России // Стандарты и качество. 2018. № 5. С. 66-70.
16. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения // М.: Федеральное агентство по техническому регулированию и метрологии. 2006. 12 с.
17. ГОСТ Р 56546–2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. 2016. 8с.
18. Коцыняк М.А., Кулешов И.А., Кудрявцев А.М., Лаута О.С. Киберустойчивость ИТКС. СПб, 2015 г.
19. Каталог национальных стандартов Росстандарт: [Электронный ресурс]. М., 2022. URL: https://www.rst.gov.ru/portal/gost/home/standarts/catalognational. (Дата обращения: 16.01.2023).
20. International Organization for Standardization. [Электронный ресурс]. URL: https://www.iso.org/ru/standards-catalogue/browse-by-ics.html. (Дата обращения: 16.01.2023).

References

1. On the approval of the Manual on the technical operation of communications and automation of territorial bodies of the Ministry of Internal Affairs of the Russia: Order 30.11.2016 No.772 . Information and legal portal of the ConsultantPlus system. – Access mode: http://base.consultant.ru (16.01.2023). (In Russ)
2. On the 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 No. 21 dated 02/18/2013. Information and legal portal of the ConsultantPlus system. – Access mode: http://base.consultant.ru (accessed: 16.01.2023). (In Russ)

3. On approval of the Requirements for the protection of information that does not constitute a state secret contained in state information systems: Order of the FSTEC of Russia dated 11.02.2013 No17. Information and Legal portal of the ConsultantPlus system. Access mode: http://base.consultant.ru (date of application: 16.01.2023). (In Russ)
4. FSTEC of Russia. Guidance document. Automated systems. Protection against unauthorized access to information. Classification of automated systems and information security requirements. (In Russ)
5. GOST R 15408-2013. Methods and means of ensuring security. Criteria for assessing the security of information technologies // Moscow: Standartinform. 2014; 152. (In Russ)
6. GOST R 53114-2008. Information protection. Ensuring information security in the organization. Basic terms and definitions. 2008; 22. (In Russ)
7. 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)
8. Guidance 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. 06/19/2002. (In Russ)
9. Methodology for determining threats to information security in information systems: approved by the FSTEC of Russia 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 (accessed: 16.01.2023). (In Russ)
10. Data bank of information security threats: [Electronic resource]. FSTEC of Russia. URL: https://bdu.fstec.ru. (Date of application: 16.01.2023). (In Russ)
11. FSTEC of Russia. Guidance document. Protection against unauthorized access to information. Terms and definitions. 2015. (In Russ)
12. National Vulnerability Database (NVD) CVE-2022-38392: [Electronic resource] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38392. (Accessed: 16.01.2023)
13. Livshits I.I. Method of assessing the security of cloud IT components according to the criteria of existing standards . *Proceedings of SPIIRAN*. 2020; 19(2): 383-411. (In Russ)
14. Livshits I.I., Neklyudov A.V. Sovereign information technologies of Russia. *Standards and quality*. 2018;. 4: 68-72. (In Russ)
15. Livshits I.I., Neklyudov A.V. Sovereign information technologies of Russia *Standards and quality*. 2018;. 5:66-70. (In Russ)
16. GOST R 50922-2006. Information protection. Basic terms and definitions. Moscow: Federal Agency for Technical Regulation and Metrology. 2006;12. (In Russ)
17. GOST R 56546-2015. Information protection. Vulnerabilities of information systems. Classification of vulnerabilities of information systems. 2016;8. (In Russ)
18. Kotsynyak M.A., Kuleshov I.A., Kudryavtsev A.M., Lauta O.S. Cyberstability of ITCS. St. Petersburg, 2015. (In Russ)
19. Catalog of national standards ROSSTANDART: [El.Res.]. Moscow, 2022. URL: https://www.rst.gov.ru/portal/gost/home/standarts/catalognational. (Accessed: 16.01.2023). (In Russ)
20. International Organization for Standardization. [electronic resource]. URL: https://www.iso.org/ru/standards-catalogue/browse-by-ics.html. (Accessed: 16.01.2023).

Сведения об авторах:

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

Лившиц Илья Иосифович, доктор технических наук, профессор практики, Livshitz.i@yandex.ru

Мещеряков Михаил Олегович, студент; mem1201@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

Information about authors:

Alexey O. Efimov, full-time adjunct; ea.aleksei@yandex.ru

Ilya I. Livshits, Dr. Sci.(Eng.), Prof. of Practice; Livshitz.i@yandex.ru

Mikhail O. Meshcheryakov, Student; mem1201@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, full-time adjunct; romanovna_vika@inbox.ru

Конфликт интересов/Conflict of interest.

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

Поступила в редакцию/ Received 30.09.2023.

Одобрена после рецензирования/ Reviced 19.10.2023.

Принята в печать/ Accepted for publication 19.10.2023.