УДК 004.42
ББК 32.973-018.2
В 58

Власенко Александра Владимировна
Кандидат технических наук, доцент, зав. кафедрой компьютерных технологий и информационной безопасности института компьютерных систем и информационной безопасности Кубанского государственного технологического университета, Краснодар, e-mail: Alex_Vlasenko@list.ru
Егорихин Юрий Евгеньевич
Аспирант кафедры компьютерных технологий и информационной безопасности института компьютерных систем и информационной безопасности Кубанского государственного технологического университета, Краснодар, e-mail: yura.egor@rambler.ru
Клименко Ксения Викторовна
Аспирант кафедры компьютерных технологий и информационной безопасности института компьютерных систем и информационной безопасности Кубанского государственного технологического университета, Краснодар, e-mail: xeniya_super@mail.ru

Разработка программного модуля автоматизации процесса определения уровня защищенности информации в ИСПДн и ГИС

Аннотация. *Представлена разработка программного модуля, написанного на языке Java, позволяющего автоматизировать процесс формирования требований защищенности информации в информационных системах персональных данных (ИСПДн) и государственных информационных системах (ГИС) в соответствии с требованиями ФСТЭК России.*

Ключевые слова: *информационная безопасность, защита информации, уровень защищенности, автоматизированная система, угроза безопасности, информационная система персональных данных, объект информатизации.*

Vlasenko Aleksandra Vladimirovna
Candidate of Technical Sciences, Associate Professor, Head of Computer Technologies and Information Security Department, Institute of Computer Systems and Information Security, Kuban State University of Technology, Krasnodar, e-mail: Alex_Vlasenko@list.ru
Egorikhin Yuriy Evgenyevich
Post-graduate student of Computer Technologies and Information Security Department, Institute of Computer Systems and Information Security, Kuban State University of Technology, Krasnodar, e-mail: yura.egor@rambler.ru
Klimenko Kseniya Viktorovna
Post-graduate student of Computer Technologies and Information Security Department, Institute of Computer Systems and Information Security, Kuban State University of Technology, Krasnodar, e-mail: xeniya_super@mail.ru

Development of the program module of automation of the process of determining the level of information protection in information systems of personal data and in state information systems

Abstract. *The paper presents the development of the program module written in the Java language, allowing automation of the formation of requirements of information security in the information systems of personal data (ISPD) and in the state information systems (SIS) according to requirements of FSTEC of Russia.*

Keywords: *information security, information protection, level of security, automated system, security threat, information system of personal data, information object.*

Одной из наиболее серьезных проблем, затрудняющих применение современных информационных технологий, является обеспечение информационной безопасности персональных данных. Работы по защите информации в Российской Федерации ведутся интенсивно и достаточно продолжительное время. Накоплен существенный опыт. На сегодняшний день уже недостаточно для обеспечения безопасности провести на предприятии ряд организационных мероприятий, включить в состав автоматизированных систем некоторые технические и программные средства.

Главное направление поиска новых путей защиты информации представляет собой реализацию регулярного процесса, осуществляемого на всех этапах жизненного цикла систем обработки информации при комплексном использовании всех имеющихся средств защиты. При этом все средства, методы и мероприятия, используемые для защиты информации,

наиболее рациональным образом объединяются в единый целостный механизм, причем не только от злоумышленников, но и от некомпетентных или недостаточно подготовленных пользователей и персонала, а также нештатных ситуаций технического характера.

Важнейшим аспектом проблемы обеспечения безопасности компьютерных систем является определение, анализ и классификация возможных угроз безопасности автоматизированной системы (АС).

Перечень значимых угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для проведения анализа рисков и формулирования требований к системе зашиты АС.

Для автоматизации процесса определения уровня защищенности информации в ИСПДн и ГИС был разработан программный модуль, написанный на языке высокого уровня Java (рис. 1).

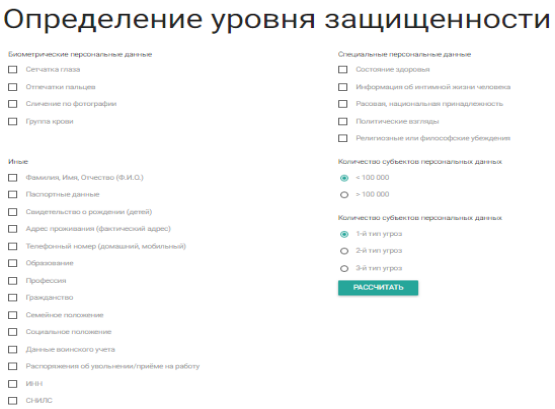


Рис. 1. Программный модуль определения уровня защищенности

В зависимости от типа обрабатываемых в системе персональных данных, а также количества субъектов персональных данных программный модуль производит расчет уровня защищенности (рис. 2).

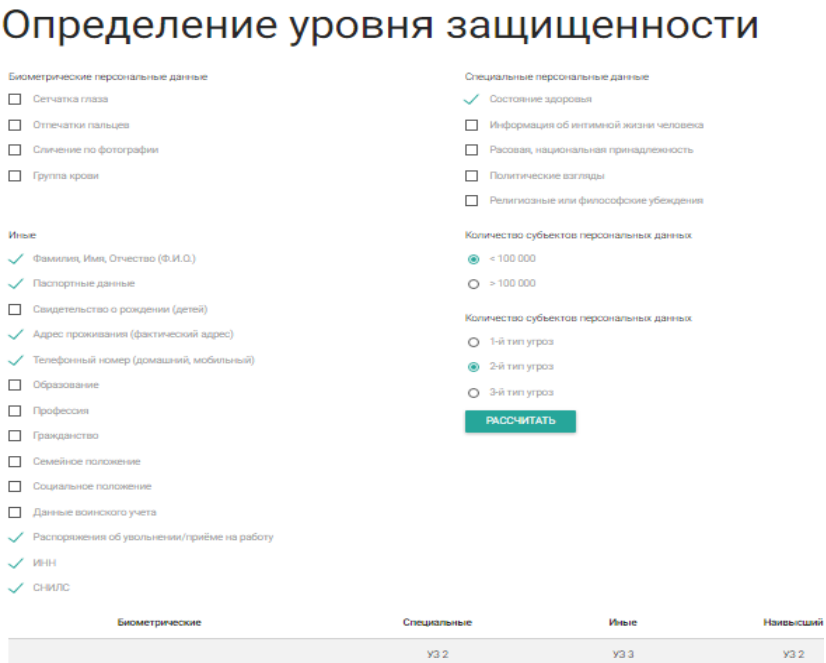
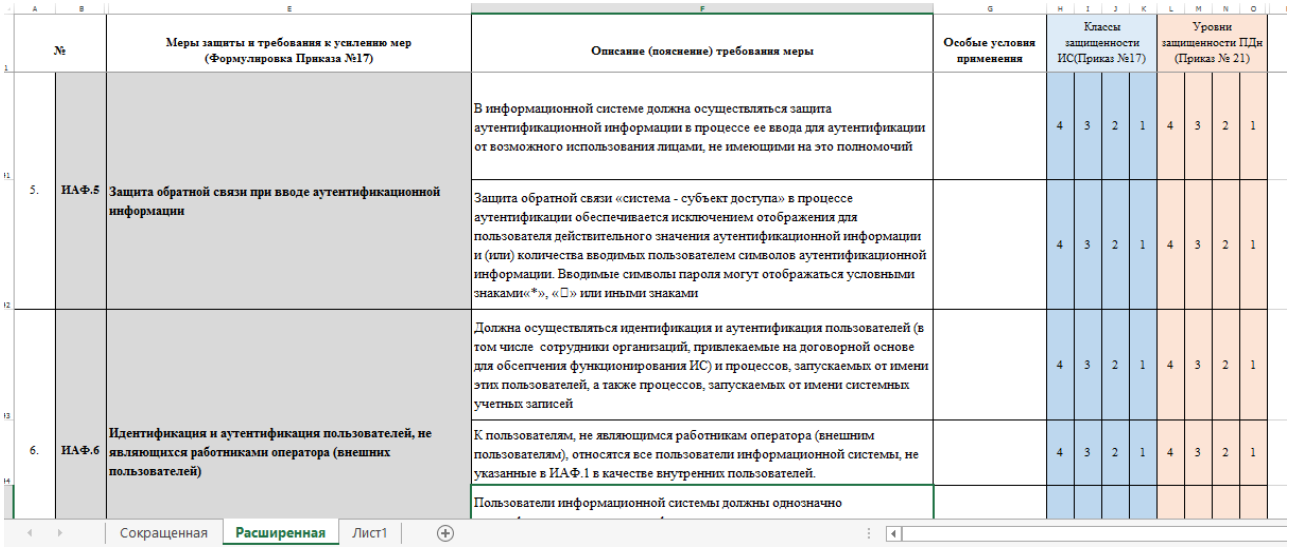


Рис. 2. Расчет уровня защищенности

Для формирования требований защищенности информации в ИСПДн и ГИС используется ранее созданная база данных, опирающаяся на приказы Федеральной службы по техническому и экспортному контролю (ФСТЭК). На рисунке 3 представлена переработанная база данных на основании приказа ФСТЭК России от 18.02.2013 N 21 [1].

В разработанной базе данных существует возможность выборки мер защиты информации в соответствии с указанной информацией. После определения уровня защищенности в

ИСПДн или класса защищенности в ГИС появляется возможность автоматизированного определения необходимых мер защиты [2, 3].

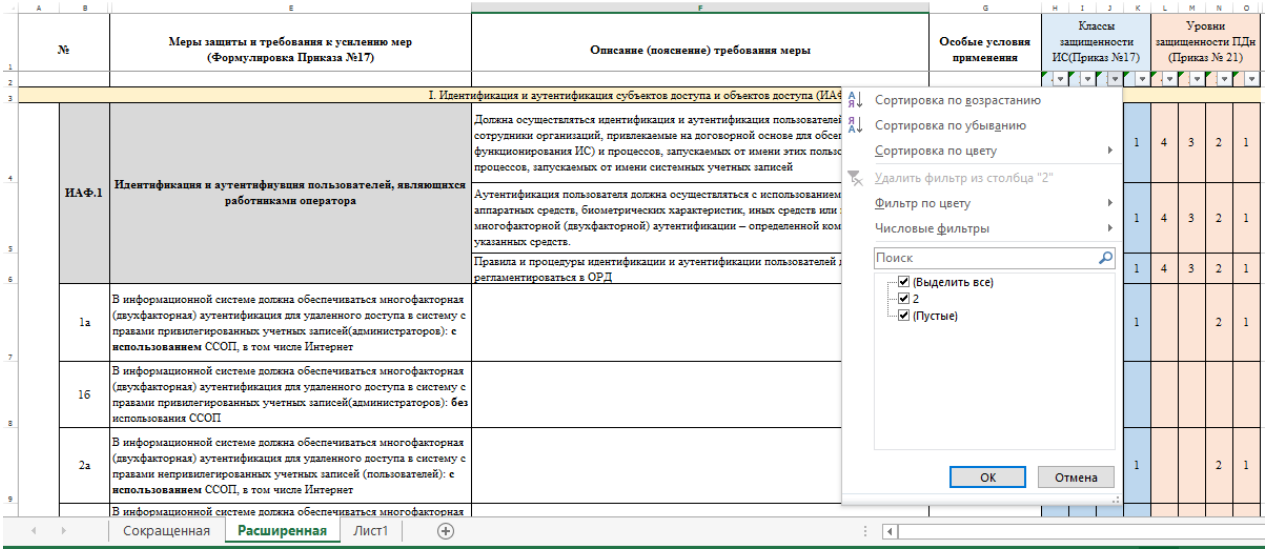


№		Меры защиты и требования к усилению мер (Формулировка Приказа №17)	Описание (пояснение) требования меры	Особые условия применения	Классы защищенности ИС(Приказ №17)				Уровни защищенности ПДн (Приказ № 21)			
5.	ИАФ.5	**Защита обратной связи при вводе аутентификационной информации**	В информационной системе должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий		4	3	2	1	4	3	2	1
			Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками«*», «□» или иными знаками		4	3	2	1	4	3	2	1
6.	ИАФ.6	**Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)**	Должна осуществляться идентификация и аутентификация пользователей (в том числе сотрудники организаций, привлекаемые на договорной основе для обеспечения функционирования ИС) и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей		4	3	2	1	4	3	2	1
			К пользователям, не являющимся работникам оператора (внешним пользователям), относятся все пользователи информационной системы, не указанные в ИАФ.1 в качестве внутренних пользователей.		4	3	2	1	4	3	2	1
			Пользователи информационной системы должны однозначно									

Сокращенная | Расширенная | Лист1

Рис. 3. Автоматизированная база данных процессов выборки

На рис. 4 и 5 представлена выборка мер защиты и требований к необходимым мерам в зависимости от класса или уровня защищенности [4].

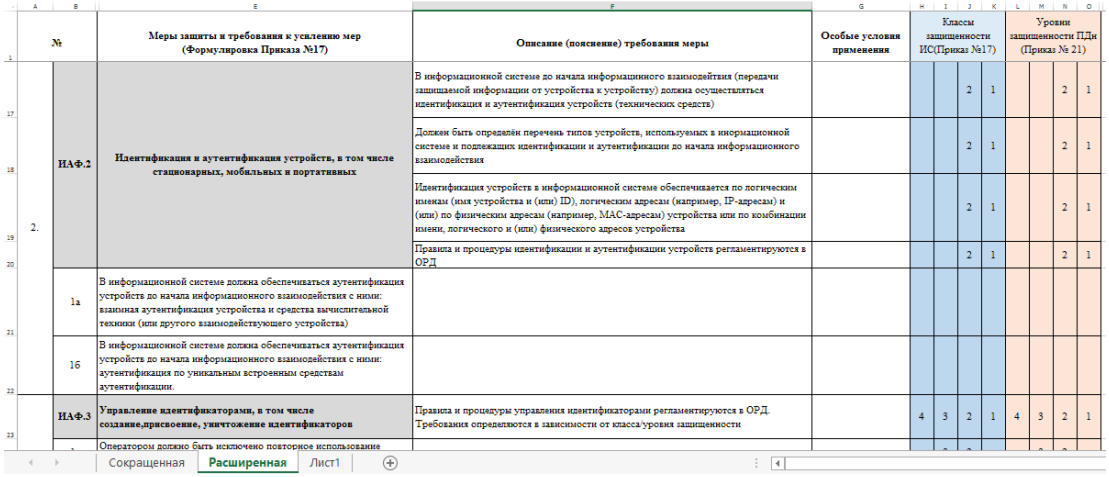


№		Меры защиты и требования к усилению мер (Формулировка Приказа №17)	Описание (пояснение) требования меры	Особые условия применения	Классы защищенности ИС(Приказ №17)				Уровни защищенности ПДн (Приказ № 21)			
		I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ										
	ИАФ.1	**Идентификация и аутентифицирующая пользователей, являющихся работниками оператора**	Должна осуществляться идентификация и аутентификация пользователей (сотрудники организаций, привлекаемые на договорной основе для обеспечения функционирования ИС) и процессов, запускаемых от имени этих пользователей, а процессов, запускаемых от имени системных учетных записей					1	4	3	2	1
			Аутентификация пользователя должна осуществляться с использованием аппаратных средств, биометрических характеристик, иных средств или многофакторной (двухфакторной) аутентификации – определенной ком указанных средств.					1	4	3	2	1
			Правила и процедуры идентификации и аутентификации пользователей регламентироваться в ОРД					1	4	3	2	1
	1а	В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами привилегированных учетных записей(администраторов): с **использованием** ССОП, в том числе Интернет						1			2	1
	1б	В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами привилегированных учетных записей(администраторов): без использования ССОП										
	2а	В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами непривилегированных учетных записей (пользователей): с **использованием** ССОП, в том числе Интернет						1			2	1
		В информационной системе должна обеспечиваться многофакторная										

Сортировка по возрастанию
Сортировка по убыванию
Сортировка по цвету
Удалить фильтр из столбца "2"
Фильтр по цвету
Числовые фильтры
Поиск
(Выделить все)
2
(Пустые)
ОК
Отмена

Сокращенная | Расширенная | Лист1

Рис. 4. Выборка мер защиты и требований к необходимым мерам в зависимости от класса или уровня защищенности



№		Меры защиты и требования к усилению мер (Формулировка Приказа №17)	Описание (пояснение) требования меры	Особые условия применения	Классы защищенности ИС(Приказ №17)				Уровни защищенности ПДн (Приказ № 21)			
2.	ИАФ.2	**Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных**	В информационной системе до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств)				2	1			2	1
			Должен быть определён перечень типов устройств, используемых в информационной системе и подлежащих идентификации и аутентификации до начала информационного взаимодействия				2	1			2	1
			Идентификация устройств в информационной системе обеспечивается по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства				2	1			2	1
			Правила и процедуры идентификации и аутентификации устройств регламентируются в ОРД				2	1			2	1
	1а	В информационной системе должна обеспечиваться аутентификация устройств до начала информационного взаимодействия с ними: взаимная аутентификация устройства и средства вычислительной техники (или другого взаимодействующего устройства)										
	1б	В информационной системе должна обеспечиваться аутентификация устройств до начала информационного взаимодействия с ними: аутентификация по уникальным встроенным средствам аутентификации.										
	ИАФ.3	**Управление идентификаторами, в том числе создание,присвоение, уничтожение идентификаторов**	Правила и процедуры управления идентификаторами регламентируются в ОРД. Требования определяются в зависимости от класса/уровня защищенности		4	3	2	1	4	3	2	1
			Оператором должно быть исключено повторное использование									

Сокращенная | Расширенная | Лист1

Рис. 5. Выборка мер, представленная в табличном виде

Выводы. Разработка программного модуля уменьшает затраты времени на определение уровня защищенности информации для ИСПДн и ГИС, автоматизировав данный процесс, а также дает возможность самостоятельного определения и формирования требований без привлечения фирм, специализирующихся на проведении мероприятий по определению уровня защищенности и формирования мер, необходимых для защиты информации.

Примечания:

1. 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 N 21. URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/691 (дата обращения: 13.10.2017).
2. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 01.11.2012 N 1119. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=137356&fld=134&dst=1000000001,0&rnd=0.7575676342131048#0 (дата обращения: 13.10.2017).
3. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11.02.2013 N 17 (ред. от 15.02.2017). URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (дата обращения: 13.10.2017).
4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России от 15 февраля 2008 г. URL: http://fstec.ru/component/attachments/download/289 (дата обращения: 13.10.2017).

References:

1. On approval of the set and content of organizational and technical measures to ensure the security of personal data when processing them in personal data information systems: order of the FSTEC of Russia dated by February 18, 2013 N 21. URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/691691 (access date: 13.10.2017).
2. On approval of the requirements for the protection of personal data when processing them in personal data information systems: Government Decree of 01.11.2012 N 1119. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=137356&fld=134&dst=1000000001,0&rnd=0.7575676342131048#0 (access date: 13.10.2017).
3. On approval of the requirements for the protection of information not constituting a state secret contained in state information systems: order of the FSTEC of Russia of 11.02.2013 N 17 (as amended on 15.02.2017). URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (access date: 13.10.2017).
4. The basic model of threats to the security of personal data when they are processed in personal data information systems: the order of the FSTEC of Russia dated by February 15, 2008. URL: http://fstec.ru/component/attachments/download/289 (access date: 13.10 .2017).