УДК 004.62

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ФОРМИРОВАНИЯ ТРЕБОВАНИЙ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ИСПДН И ГИС В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФСТЭК РОССИИ

А.В. ВЛАСЕНКО, Ю.Е. ЕГОРИХИН, К.В. КЛИМЕНКО, Е.И. КАШИРИНА

Кубанский государственный технологический университет
350072, Российская Федерация, г.Краснодар, ул.Московская, 2,
электронная почта:Vlasenko@kubstu.ru, elivkashir@yandex.ru

Разработка базы данных, позволяющей 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: угроза безопасности информации, ИСПДн, база данных.

Становление информационного общества связано с широким распространением персональных компьютеров, построением глобальной информационной Сети и подключения к ней большого числа пользователей. Эти достижения должны коренным образом изменить жизнь общества, выдвинув на передний план деятельность, связанную с производством, потреблением, трансляцией и хранением информации.

Одной из наиболее серьезных проблем, затрудняющих применение информационных технологий, является обеспечение информационной безопасности.

Информационная безопасность - такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних угроз, а с другой - её функционирование не создаёт информационных угроз для элементов самой системы и внешней среды.

Работы по защите информации у нас в стране ведутся достаточно интенсивно и уже продолжительное время. Накоплен существенный опыт. Сейчас уже никто не думает, что достаточно провести на предприятии ряд организационных мероприятий, включить в состав автоматизированных систем

некоторые технические и программные средства — и этого будет достаточно для обеспечения безопасности.

Главное направление поиска новых путей защиты информации заключается не просто в создании соответствующих механизмов, а 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.

Угроза безопасности информации - совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации или несанкционированными и непреднамеренными воздействиями на нее.

Одним из важнейших аспектов 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 формирования требований защищенности информации в ИСПДн и ГИС была создана база данных, опираясь на документыФедеральной службы по техническому и экспортному контролю (ФСТЭК). База данных представлена на рисунке 1[1].

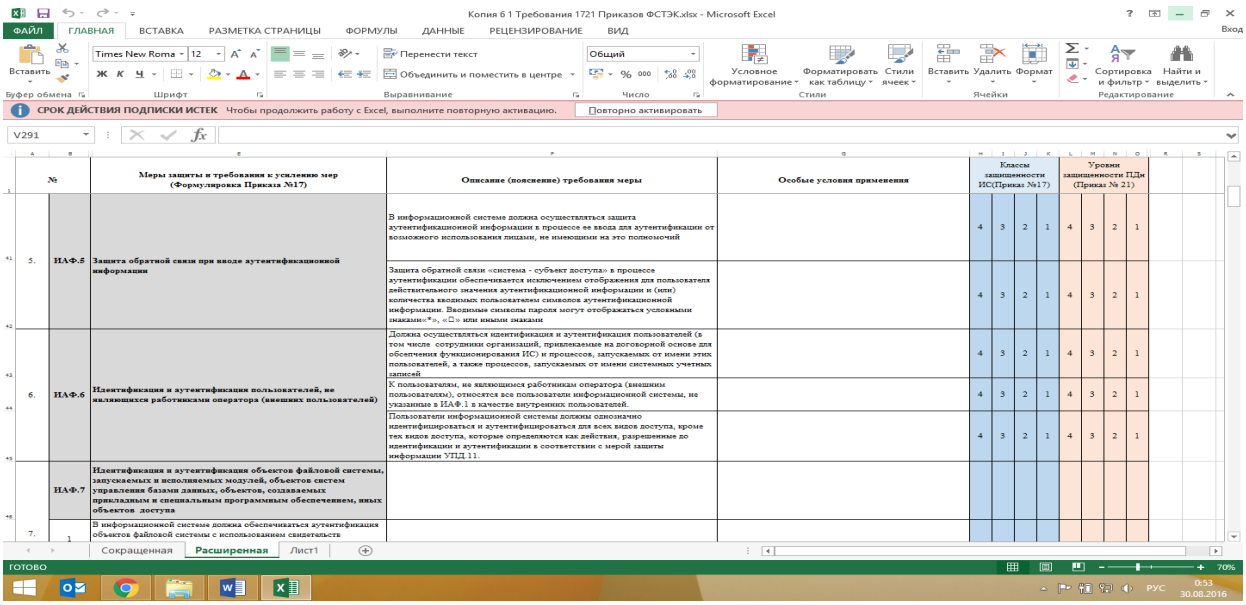

Рисунок 1 – база данных, автоматизирующая процесс выборки

Также существует возможность выборки мер защиты информации, в соответствии с защищаемой информацией. После определения уровня защищенности в ИСПДн или класса защищенности в ГИС появляется возможности автоматизированного определения необходимых мер защиты.

На рисунке 2 представлена выборка мер защиты и требований к необходимым мерам, в зависимости от класса или уровня защищенности. [2]

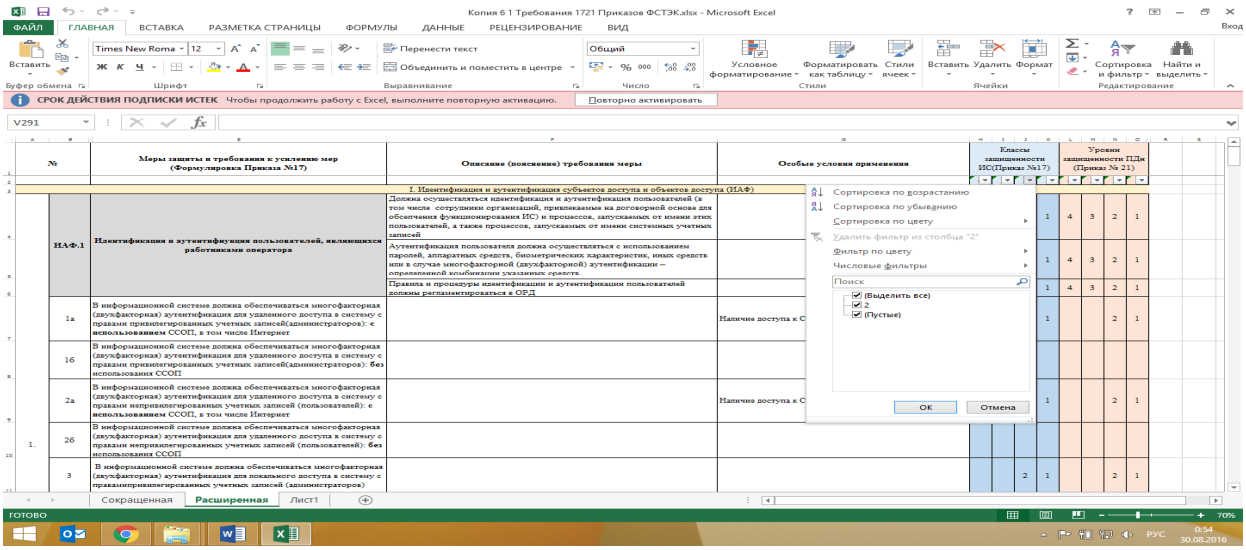

Рисунок 2 - Выборка мер защиты и требований к необходимым мерам, в зависимости от класса или уровня защищенности

На рисунке 3 показана выборка мер, представленная в табличном виде.

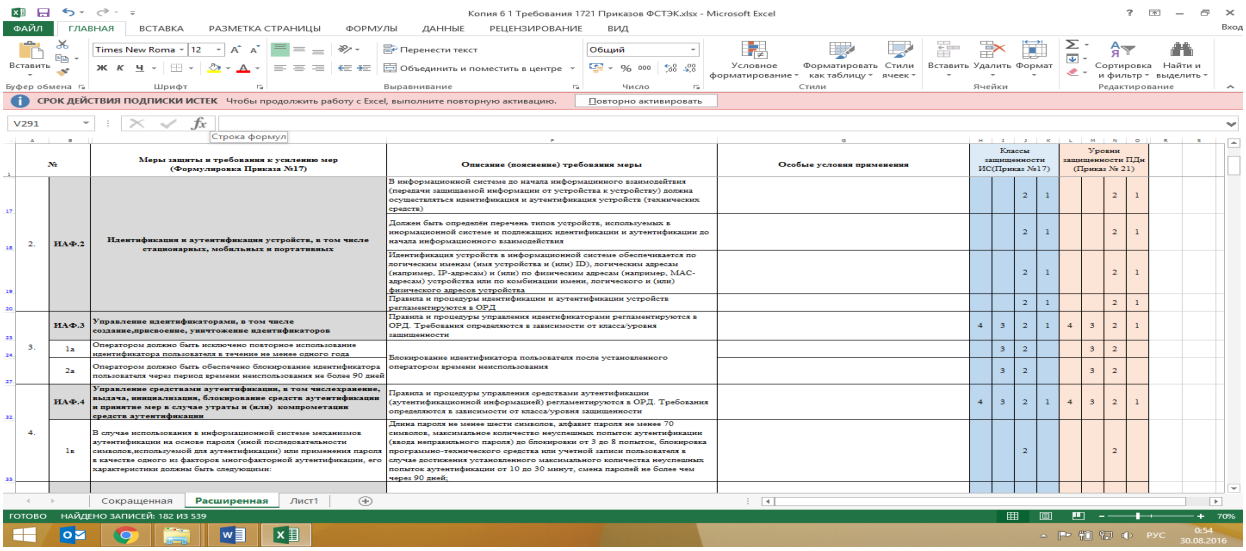

Рисунок 3 - Выборка мер, представленная в табличном виде

Исходя из вышесказанного, можно сделать вывод о том, чторазработка базы данных уменьшает затраты времени на определение угроз безопасности информации для ИСПДн и ГИС.

ЛИТЕРАТУРА

1. Приказ ФСТЭК России от 14 февраля 2008 г. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

2. Приказ ФСТЭК России от 15 февраля 2008 г. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

REFERENCES

1. Prikaz FSTEK Rossii ot 14 fevralya 2008 g. «Metodika opredeleniya aktualnykh ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh».

2. Prikaz FSTEK Rossii ot 15 fevralya 2008 g. «Bazovaya model ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh».

AUTOMATION OF PROCESSES OF FORMATION OF REQUIREMENTS OF SECURITY OF INFORMATION IN PDIS AND SIS, ACCORDING TO REQUIREMENTS OF FSTEC OF RUSSIA

A.V. VLASENKO, YU.E. EGORIKHIN, K.V. KLIMENKO, E.I. KASHIRINA

Kuban State Technological University,
2, Moskovskaya st., Krasnodar, Russian Federation, 350072;
e-mail: Vlasenko@kubstu.ru, elivkashir@yandex.ru

Development of the database allowing to automate process of formation of requirements of security of information in information systems of personal data (PDIS) and the state information systems (SIS) according to requirements of FSTEC of Russia.
Key words: threat to security of information, PDIS, database.