

*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 защиты АС.

Для автоматизации процесса формирования требований защищенности информации в ИСПДн и ГИС была создана база данных, опираясь на документы Федеральной службы по техническому и экспортному контролю (ФСТЭК). База данных представлена на рисунке 1[1].

№	Меры защиты и требования к условиям мер (Формулировка Приказа №17)	Описание (поисковая) требования меры	Особые условия применения	Классы защищенности ИС(Приказ №17)				Уровни защищенности ПДн (Приказ № 21)			
5.	И.А.Ф.6 Защита обратной связи при вводе аутентификационной информации	В информационной системе должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от несанкционированного доступа, не зависящего от этого процессинга		4	3	2	1	4	3	2	1
6.	И.А.Ф.6 Идентификация и аутентификация пользователей, не являющихся рабочими операторами (внешних пользователей)	Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается использованием отобразившейся 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
7.	И.А.Ф.7 Идентификация и аутентификация объектов файловой системы, подключаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых подключаемым и специальным программным обеспечением, иных объектов доступа	Допускается осуществлять идентификацию и аутентификацию пользователей (в том числе сотрудников 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

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 возможность 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]

№	Меры защиты и требования к условиям мер (Формулировка Приказа №17)	Описание (поисковая) требования меры	Особые условия применения	Классы защищенности ИС(Приказ №17)				Уровни защищенности ПДн (Приказ № 21)					
И.А.Ф.1	Идентификация и аутентификация пользователей, являющихся рабочими операторами	Идентификация и аутентификация субъектов доступа и объектов доступа (И.А.Ф.6)		1	4	3	2	1	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	Аутентификация пользователей должна осуществляться с использованием парольной, аппаратной, биометрической, биометрической, иных средств или в случае многофакторной (двухфакторной) аутентификации – традиционной комбинации указанных средств	Матрица доступа к С	1	1	1	1	1	1	1	1	1	1
16	В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами привилегированных учетных записей(администраторов); без использования ССОП	Аутентификация пользователей должна осуществляться с использованием парольной, аппаратной, биометрической, биометрической, иных средств или в случае многофакторной (двухфакторной) аутентификации – традиционной комбинации указанных средств	Матрица доступа к С	1	1	1	1	1	1	1	1	1	1
2а	В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами непривилегированных учетных записей (пользователей); с использованием ССОП	Аутентификация пользователей должна осуществляться с использованием парольной, аппаратной, биометрической, биометрической, иных средств или в случае многофакторной (двухфакторной) аутентификации – традиционной комбинации указанных средств		1	1	1	1	1	1	1	1	1	1
26	В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами непривилегированных учетных записей (пользователей); без использования ССОП	Аутентификация пользователей должна осуществляться с использованием парольной, аппаратной, биометрической, биометрической, иных средств или в случае многофакторной (двухфакторной) аутентификации – традиционной комбинации указанных средств		1	1	1	1	1	1	1	1	1	1
3	В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами привилегированных учетных записей (администраторов)	Аутентификация пользователей должна осуществляться с использованием парольной, аппаратной, биометрической, биометрической, иных средств или в случае многофакторной (двухфакторной) аутентификации – традиционной комбинации указанных средств		2	1	1	1	1	2	1	1	1	1

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.

№	Меры защиты и требования к условиям мер (Формулировка Приказа №17)	Описание (поискать) требования меры	Особые условия применения	Классы защищенности ИС (Приказ №17)		Уровни защищенности ПДн (Приказ № 21)					
				1	2	1	2				
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 (физических устройств). Должна быть обеспечена проверка типов устройств, используемых в информационной системе и подлинности идентификации и аутентификации до начала информационного взаимодействия. Идентификация устройств в информационной системе обеспечивается по логическим именам (имя устройства и (или) IP), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-адресам) устройств или по комбинации имени, логического и (или) физического адресов устройства. Правила и процедуры идентификации и аутентификации устройств регламентируются в ОРД.			2	1	2	1			
3	Управление идентификаторами, в том числе создаваемыми, учетными идентификаторами	Оператором должно быть обеспечено повторное использование идентификатора пользователя в течение не менее одного года. Оператором должно быть обеспечено блокирование идентификатора пользователя через период времени неиспользования не более 90 дней.	Блокирование идентификатора пользователя после установленного оператором времени неиспользования								
4	Управление средствами аутентификации, в том числе паролями, ключами, аппаратными блоками аутентификации и принятию мер в случае утраты и (или) компрометации средств аутентификации.	Правила и процедуры управления средствами аутентификации (аутентификационной информацией) регламентируются в ОРД. Требования определяются в зависимости от класса/уровня защищенности. Длина пароля не менее шести символов, алфавит пароля не менее 70 символов, максимальное количество успешных попыток аутентификации (слова неправильного пароля) до блокировки от 3 до 8 попыток. Блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества успешных попыток аутентификации от 10 до 30 минут, смена паролей не более чем через 90 дней.	Правила и процедуры управления средствами аутентификации (аутентификационной информацией) регламентируются в ОРД. Требования определяются в зависимости от класса/уровня защищенности.	4	3	2	1	4	3	2	1

Рисунок 3 - Выборка мер, представленная в табличном виде

Исходя из вышесказанного, можно сделать вывод о том, что разработка 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.