Научные труды КубГТУ, № 16, 2016 год

УДК 004.056

АНАЛИЗ ХАРАКТЕРИСТИК ОПРЕДЕЛЕНИЯ НАРУШИТЕЛЯ ПРИ МОДЕЛИРОВАНИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

А.В. ВЛАСЕНКО, Р.В. ЖУК

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

Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю Российской Федерации (далее – ФСТЭК России) при выборе угроз информационной безопасности устанавливает 6 типов нарушителей информационной безопасности с различным потенциалом. Данные типы нарушителя разделяются по следующим критериям: доступ в контролируемую зону (внешний и внутренний нарушитель), возможности нарушителя (потенциал). Вышеперечисленная методика противоречит действующей, утвержденной Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Ключевые слова: модель угроз, угроза информационной безопасности, нарушитель, потенциал, персональные данные, информационная система персональных данных.

В соответствии с Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее – Базовая модель) классификация нарушителя информационной безопасности (далее - нарушитель) приводится относительно возможности доступа к активам информационной системы и делится на 2 типа [1]:

1. Внешний:

– разведывательные службы государств;

– криминальные структуры;

– конкуренты (конкурирующие организации);

– недобросовестные партнеры;

– внешние субъекты (физические лица).

2. Внутренний:

– лица, имеющие санкционированный доступ к информационной системе персональных данных(далее – ИСПДн), но не имеющие доступа к персональным данным (далее – ПДн);

– зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места;

– зарегистрированные пользователи, осуществляющие удаленный доступ к ПДн по локальным и (или)распределенным информационным системам;

– зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента;

– системный администратор;

– администратор безопасности;

– программисты-разработчики;

– разработчики, лица, осуществляющие аутсорсинг.

Данная градация противоречит используемой Банком данных угроз безопасности информации, который в свою очередь, применяет планируемую к утверждению методику определения угроз безопасности информации в информационных система. Проект методики опубликован на сайте ФСТЭК России, но на данный момент изъят из общего доступа. Согласно методике, нарушитель аналогично Базовой модели делится на 2 типа [2]:

1. Внешний:

– специальные службы иностранных государств (блоков государств);

– террористические, экстремистские группировки;

– преступные группы (криминальные структуры);

– внешние субъекты (физические лица);

– конкурирующие организации;

– разработчики, производители, поставщики программных, технических и программно-технических средств;

– бывшие работники (пользователи).

2. Внутренний:

– лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики т.д.);

– пользователи информационной системы;

– администраторы информационной системы и администраторы безопасности.

В дополнение к описанным аналогично Базовой модели угроз возможностям, нарушитель имеет характеристику «потенциал» (со следующими значениями «низкий», «средний», «высокий»).

Потенциал нарушителя заранее определен и представлен в таблице 1.

Таблица 1 – Потенциал нарушителя

Нарушитель	Потенциал
Разведывательные службы государств	Высокий
Криминальные структуры	Средний
Террористические, экстремистские группировки	Средний
Конкуренты (конкурирующие организации)	Средний
Внешние субъекты (физические лица)	Низкий
Пользователи ИСПДн	Низкий
Системны администратор и администратор безопасности	Средний
Разработчики, лица, осуществляющие аутсорсинг	Средний
Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Низкий
Лица, обеспечивающие функционирование ИСПДн или обслуживающие инфраструктуру оператора	Низкий
Бывшие работники(пользователи)	Низкий

Таким образом, сопоставим нарушителей, представленных в базовой модели с нарушителями, приведенными в проекте методики, и получим таблицу 2.

Таблица 2 – Сравнение методик

Нарушитель	Методический документ	
	Базовая модель ИСПДн	Методика определения угроз безопасности ИС
Разведывательные службы государств	Внешний	Внешний, внутренний
Криминальные структуры	Внешний	Внешний
Террористические, экстремистские группировки		Внешний
Конкуренты (конкурирующие организации)	Внешний	Внешний
Недобросовестные партнеры	Внешний	
Внешние субъекты (физические лица)	Внешний	Внешний
Должностные лица, обеспечивающие нормальное функционирование ИСПДн	Внутренний	
Зарегистрированные пользователи с ограниченным доступом	Внутренний	
Пользователи ИСПДн		Внутренний
Зарегистрированные пользователи с удаленным доступом	Внешний	
Системны администратор	Внутренний	Внутренний
Администратор безопасности	Внутренний	
Программисты-разработчики ППО	Внутренний	Внешний
Разработчики, лица, осуществляющие аутсорсинг	Внутренний	
Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ		Внешний
Лица, обеспечивающие функционирование ИСПДн или обслуживающие инфраструктуру оператора		Внешний
Бывшие работники(пользователи)		Внешний

Из таблицы 2 следует, что при определении угроз информационной безопасности упразднены следующие категории нарушителей:

– Недобросовестные партнеры;
– Зарегистрированные пользователи с ограниченным доступом;
– Зарегистрированные пользователи с удаленным доступом.

Также, категории «Системный администратор» и «Администратор безопасности» объединены, что приведет к объединению возможных угроз, реализуемых данными категориями нарушителей.

Категория «Должностные лица, обеспечивающие нормальное функционирование ИСПДн» разделена на категории «Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ» и «Лица, обеспечивающие функционирование ИСПДн или обслуживающие инфраструктуру оператора», а также перенесена из «внутреннего» типа нарушителя во «внешний», что приводит к изменению угроз информационной безопасности, реализуемых данной категорией.

В результате, при использовании Банка данных угроз безопасности информации ФСТЭК России, на первом этапе необходимо выявить категории нарушителей согласно Базовой модели. Далее, сопоставить выработанный перечень нарушителей с таблицей 2, для актуализации выявленных категорий нарушителя. И на заключительном этапе, актуализированные категории нарушителей, в соответствии с таблицей 1, сопоставить с потенциалом.

Таким образом, введение в эксплуатацию банка данных угроз безопасности информации ФСТЭК России без утверждения обновленной методики значительно увеличивает количество итераций в алгоритме определения нарушителя. Что, существенно влияет на определение перечня угроз информационной безопасности активов ИСПДн.

ЛИТЕРАТУРА

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утв. зам. дир.

ФСТЭК России 15 февраля 2008 г. [Электронный ресурс] // http://fstec.ru/component/attachments/download/289

2. Методический документ: Методика определения угроз безопасности информации в информационных системах. Проект ФСТЭК России [Электронный ресурс] // http://fstec.ru/component/attachments/download/812

REFERENCES

1. Bazovaya model ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh. Utv. zam. dir. FSTEK Rossii 15 fevralya 2008 g. [Elektronnyy resurs] // http://fstec.ru/component/attachments/download/289

2. Metodicheskiy dokument: Metodika opredeleniya ugroz bezopasnosti informatsii v informatsionnykh sistemakh. Proekt FSTEK Rossii [Elektronnyy resurs] // http://fstec.ru/component/attachments/download/812

ANALYSIS OF CHARACTERISTICS DEFINITIONS INTRUDERS THREAT MODELING INFORMATION SECURITY IN THE PERSONAL DATA INFORMATION SYSTEMS

A.V. VLASENKO, R.V. ZHUK

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

When security specialists selecting information from Bank of data security threats to the Federal Service for Technical and Export Control of the Russian Federation (hereinafter - FSTEC Russia), security threats establishes 6 types of information security intruder with a different potential. These types of intruder classified by the following criteria: access to the controlled area (outside and inside the intruder), the possibility of the intruder (potential). Method listed above is contrary to the current approved basic model of personal data security threats at their processing within the information systems of personal data.
Key words: threat model threat to information security, the intruder, the potential of personal data, personal data information systems.