УДК 004.056

***А.А. Бутин*[1], *Е.В. Иванова*[1]**

[1]*Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация*

МЕТОДИЧЕСКИЕ АСПЕКТЫ ПОСТРОЕНИЯ МОДЕЛЕЙ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ МУНИЦИПАЛЬНЫХ ОРГАНОВ ВЛАСТИ

Аннотация. *В статье рассматриваются основы построения модели угроз информационной безопасности. Приводятся основные этапы в процессе построения, нормативно-правовая документация и электронные ресурсы, призванные упростить построение модели. Рассматриваются особенности использования методологии моделирования угроз в информационных системах, функционирующих в муниципальных органах власти.*

Ключевые слова: *модель угроз, безопасность информации, система защиты информации, государственная тайна.*

***A.A. Butin*[1], *E.V. Ivanova*[1]**

[1]*Irkutsk State Transport University, Irkutsk, Russia*

MODEL OF THREATS OF INFORMATION SECURITY FOR MUNICIPAL AUTHORITIES

Annotation. *This article discusses the basics of building a model of information security threats. It discusses the main stages in the construction process, the regulatory documents and electronic resources designed to simplify the construction of the model. The features of using the methodology of modeling threats in information systems operating in municipal authorities are considered.*

Key words: *model of threats, information security, information security system, state secret*

В настоящее время много внимания уделяется информационной безопасности, в частности, таким ее аспектам, как организационные меры, призванные стать первым рубежом в построении системы защиты информации. Грамотно проведенные первые шаги являются основой для создания полной и эффективной комплексной системы защиты. Поэтому важно уделить особое внимание построению модели угроз информационной безопасности (далее – ИБ), которая во многом определяет будущее данной системы [1]-[5].

Стандарт СТО БР ИББС – 1.0-2014 определяет модель угроз информационной безопасности следующим образом: это описание актуальных для организации источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба».

В соответствии с этим можно сделать вывод, что модель угроз – документ, содержащий в себе описания угроз и уязвимостей информационной системы, которые могут использоваться с целью оказания негативного воздействия на информационные активы организации. Разработка модели угроз является необходимым условием формирования обоснованных требований к обеспечению безопасности информации в информационных системах (далее – ИС) и проектирования системы защиты ИС.

С применением методики построения моделей угроз решаются следующие задачи:

1. разработка частных моделей угроз безопасности в конкретных ИС с учетом их назначения, условий и особенностей функционирования;
2. анализ защищенности ИС от угроз безопасности в ходе организации и выполнения работ по защите информации;

3. разработка системы защиты, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов, предусмотренных для соответствующего класса ИС;

4. проведение мероприятий, направленных на предотвращение несанкционированного доступа к информации и (или) передачи их лицам, не имеющим права доступа к такой информации;

5. недопущение воздействия на технические средства ИС, в результате которого может быть нарушено их функционирование;

6. контроль обеспечения уровня защищенности информации.

Сам процесс построения модели представляет собой последовательность следующих операций:

– анализ защищаемой информационной системы;

– выявление источников угроз информационной безопасности;

– определение актуальных угроз безопасности информационной системы и способов их реализации.

На первом этапе требуется провести анализ информационной среды организации. Определить, какую информацию обрабатывают в организации, как производится обработка информации, какое программное обеспечение используются и т.д. Из собранной информации формируется первый раздел модели угроз «Описание информационной системы».

На втором этапе рассматриваются все возможные угрозы для информации в защищаемой ИС. В этом вопросе могут помочь электронные банки данных угроз и уязвимостей, например, банк данных угроз и уязвимостей ФСТЭК (http://bdu.fstec.ru) или Common Vulnerabilities and Exposures Database (https://www.cvedetails.com). На 29 марта 2019 года в банке данных ФСТЭК числятся более двадцати тысяч уязвимостей и более двухсот угроз.

Данный этап описывается во втором разделе модели угроз « Перечень угроз безопасности персональных данных, обрабатываемых в информационной системе»

Уязвимости в банках данных оцениваются при помощи системы CVSS. CVSS – Common Vulnerability Scoring System (Общая система оценки уязвимостей) – это система, которая позволяет осуществлять сравнение уязвимостей программного обеспечения с точки зрения их опасности.

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	959	0.90
1-2	860	0.80
2-3	4392	3.90
3-4	3882	3.50
4-5	24278	21.60
5-6	21761	19.40
6-7	15158	13.50
7-8	25396	22.60
8-9	502	0.40
9-10	15176	13.50
Total	112364	

Weighted Average CVSS Score: **6.7**

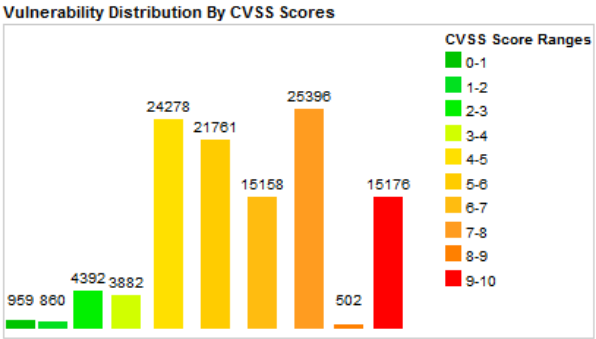

Рисунок 1. Распределение всех уязвимостей по баллам общей системы оценки уязвимостей (CVSS)

В настоящее время наибольшее распространение в практической деятельности по оценке опасности уязвимостей получила версия 2.0 общей системы оценки уязвимостей.

Оценка производится на основе базового вектора уязвимости CVSS v2.0, который представляет собой комбинированную информацию об основных метриках (критериях), представляемую в виде текстовой формализованной записи (строки) и численного значения (оценки) - AV:X/AC:X/Au:X/C:X/I:X/A:X, где

1. AV – метрика (критерий) способа получения доступа нарушителем;

2. AC – метрика (критерий) сложности получения доступа нарушителем;
3. Au – метрика (критерий) характеристики потребности нарушителя в аутентификации;
4. C – метрика (критерий) влияния на конфиденциальность;
5. I – метрика (критерий) влияния на целостность;
6. A – метрика (критерий) влияния на доступность;
7. X – значение метрики (критерия).

На третьем этапе при помощи методики ФСТЭК проводится анализ выявленных угроз и уязвимостей. Актуальные угрозы включаются в модель угроз, а неактуальные отбрасываются. Актуальной считается угроза, которая может быть реализована в ИС и представляет опасность для информации, обрабатываемой в ИС. Данный этап является третьим разделом модели угроз – «Определение актуальных угроз безопасности».

Подход к составлению перечня актуальных угроз состоит в следующем: при составлении перечня актуальных угроз безопасности информации, каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент. Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИС. Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИС, в соответствии с правилами, приведенными в таблице 1.

Таблица 1. Правила отнесения угрозы безопасности к актуальной

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная
Очень высокая	Актуальная	Актуальная	Актуальная

На основе приведенного в модели угроз перечня актуальных угроз производится выбор организационно-технических мер и средств защиты информации. Данные меры приводятся в последнем разделе модели угроз в виде таблицы.

Для муниципальных органов власти модель угроз – обязательный документ, на основе которого должна строиться система защиты информации. В современном мире в информационных системах муниципальных образований обрабатывается информация, составляющая государственную тайну, которая подлежит обязательной защите. Поэтому очень важно составить грамотную и эффективную модель угроз для информационных систем муниципалитетов.

Нужно понимать, что в информационных системах обрабатывается большое количество информации различных грифов секретности. Защитная подсистема не должна мешать данным системам эффективно работать, она должна быть достаточно гибкой и не ограничивать в действиях пользователей при обработке информации.

При выработке рекомендаций необходимо руководствоваться приказом ФСТЭК № 17 от 13.02.2013, который описывает требования к защите информации в государственных информационных системах, не составляющей государственную тайну. Это поможет в построении защиты для информационных систем, обрабатывающих персональные данные.

В отношении систем, обрабатывающих сведения, составляющие государственную тайну, следует обратиться к Закону РФ "О государственной тайне" № 5485-1 от 21.07.1993. В четвертом разделе данного закона описываются порядок доступа лиц к государственной тайне, права и ответственность за нарушение законодательства о государственной тайне. В статье 2 Закона РФ «О государственной тайне» дано определение системы защиты этой тайны:

«Под системой защиты государственной тайны понимается совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях». Исходя из этого, можно сделать вывод, что модель угроз является частью системы защиты информации, составляющей государственную тайну в части организационного мероприятия, проводимого в самом начале построения системы защиты.

Модель угроз для муниципальных органов власти по структуре мало чем отличается от частных моделей угроз, за исключением того, что в разделе рекомендаций будут находиться требования к составляющим системы защиты, которые содержатся в приказах ФСТЭК России, например, требования к межсетевым экранам утверждены приказом № 9 от 09.02.2016. Кроме того, необходимо помнить, что автоматизированные системы, как и защищаемое помещение, должны пройти обязательную аттестацию на соответствие требованиям ФСТЭК России. То же самое касается и рекомендуемых средств защиты – они обязательно должны пройти сертификацию и удовлетворять требованиям к данной информационной системе. Специфика модели будет состоять в структурно-функциональных характеристиках информационных систем, так как в них обрабатываются сведения, составляющие государственную тайну.

Поскольку в модели будут содержаться требования к подсистеме защиты для информационных систем, обрабатывающих сведения, составляющих государственную тайну, документ также будет обладать соответствующим грифом секретности.

Допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке и предусматривает принятие на себя обязательств перед государством, согласие на частичные, временные ограничения их прав, письменное согласие, ознакомление с нормами законодательства РФ и принятие решения о допуске оформляемого лица к сведениям, составляющим государственную тайну.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Стандарт ЦБР СТО БР ИББС-1.0-2014. N Р-399 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». – Введ. 2014-05-17.

2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. – Введ. 2008-02-15.

3. Банк данных угроз и уязвимостей ФСТЭК // (http://bdu.fstec.ru) // (Дата обращения – 02.04.2019).

4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. – Введ. 2008-02-14.

5. Российская Федерация. Законы. О государственной тайне [Электронный ресурс]: федер. закон от 21.07.1993 N 5485-1, ред. от 29.07.2018 – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=303613&fld=134&dst=1000000001,0&rnd=0.9554976573647225#05867016681194195 (Дата обращения – 14.04.2019).

REFERENCES

1. Standard CBR STO BR IBBS-1.0-2014 N R-399 «Ensuring the information security of organizations of the banking system of the Russian Federation. General provisions». – Fr. 2014-05-17.

2. The basic model of threats to the security of personal data during their processing in the information systems of personal data. – Fr. 2008-02-15.

3. Databank of threats and vulnerabilities FSTEC (http://bdu.fstec.ru) (date of the application – 02.04.2019).

4. Methods for determining the actual threats to the security of personal data when they are processed in personal data information systems. – Fr. 2008-02-14.

5. Russian Federation. Laws. About state secrets [Electronic resource] federal law of July 21, 1993 N 5485-1, ed. from 07.29.2018 – Access Mode: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=303613&fld=134&dst=1000000001,0&rnd=0.9554976573647225#05867016681194195 (Date of appeal – 14.04.2019).

6.

Информация об авторах

Бутин Александр Алексеевич – к.ф-м.н, доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: butin_aa@mail.ru

Иванова Елизавета Валерьевна – магистрант, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: kaileena.ivanova@yandex.ru

Author

Butin Aleksandr Alekseyevich – Ph. D. of Physical and Mathematical Sciences, Associate Professor, the Sub-department of Information Systems and Information Security, Irkutsk State Transport University, Irkutsk, e-mail: butin_aa@mail.ru

Ivanova Elizaveta Valer'evna – graduate student, Irkutsk State Trans-port University, Irkutsk, e-mail: kaileena.ivanova@yandex.ru

Для цитирования

Бутин А.А. Иванова Е.В. Методические аспекты построения моделей угроз безопасности информации для муниципальных органов власти // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2019. – №2. – С. 64-68 – Режим доступа: http://ismm-irgups.ru/toma/23-2019, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 19.06.2019)

For citation

Butin A.A. Ivanova E.V. *Metodicheskiye aspekty postroyeniya modeley ugroz bezopasnosti informatsii dlya munitsipal'nykh organov vlasti* [Model of threats of information security for municipal authorities] // *Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal* [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2019. No. 2. P. 64-68 – Access mode: http://ismm-irgups.ru/toma/23-2019, free. – Title from the screen. – Language Russian, English. [Accessed 19/06/19]