СИСТЕМАТИЗАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ УПРОЩЕНИЯ ПОСТРОЕНИЯ МОДЕЛИ УГРОЗ

SYSTEMATIZE INFORMATION SECURITY THREATS TO SIMPLIFY THREAT MODEL

УДК 004.056.53

Безродных Олег Анатольевич, старший инженер, Главный центр информационных технологий войск национальной гвардии Российской Федерации, г. Москва.

Bezrodnykh Oleg Anatolevich, Senior Engineer, Main information technology center of the National guard troops of the Russian Federation, Moscow.

Аннотация

В данной статье рассмотрены вопросы систематизации угроз безопасности информации для дальнейшего упрощения построения модели угроз безопасности информации. Для анализа и систематизации использованы данные из Банка данных угроз Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК России), отталкиваясь от которых должно производиться создание модели угроз информационной безопасности для информационной системы уже существующей или же проектируемой.

Annotation

This article discusses the issues of systematization of threats to information security to further simplify the construction of a model of threats to information security. For the analysis and systematization, data from the Threat databank of the Federal service for technical and export control of the Russian Federation (FSTEC of

Russia) were used, starting from which a model of information security threats for an existing or projected information system should be created.

Ключевые слова: угрозы безопасности информации, защита информации.

Keywords: information security threats, information protection

Введение

В настоящее время в сфере информационной безопасности используется утверждаемый и предоставляемый ФСТЭК России Банк данных угроз безопасности информации [1].

Угрозы безопасности информации (УБИ), содержащиеся в нем, используются для построения модели угроз [2]. В процессе моделирования оценивается возможность реализации каждой угрозы, ее опасность для информационной системы, последствия при реализации угрозы и в результате экспертная оценка актуальности угроз [3, 4].

Систематизация угроз безопасности позволяет изначально не рассматривать угрозы, которые не могут присутствовать в имеющихся условиях. Это позволяет упростить процесс определения актуальных УБИ и привлекать к экспертной оценке менее квалифицированных специалистов в области информационной безопасности (ИБ) .

Процесс систематизации угроз безопасности информации

В большинстве случаев систематизация угроз безопасности производится по их направленности (типу нарушения, последствиям):

- нарушение конфиденциальности;
- нарушение целостности;
- нарушение доступности.

По источнику возникновения:

- внутренний нарушитель;
- внешний нарушитель.

В данной статье предлагается систематизация УБИ по условиям эксплуатации (имеющимся или проектируемым), позволяющая производить фильтрацию актуальных УБИ.

Банк данных угроза заполняется по мере обнаружения новых угроз безопасности, сам перечень угроз практически не несет в себе определенной последовательности угроз и для специалиста мало с ним сталкивавшегося возникают трудности в оценке описанных там угроз для своего объекта защиты.

При анализе угроз из состава Банка данных угроз ФСТЭК можно произвести систематизацию перечисленных угроз. Угрозы можно разделить на две большие категории:

- постоянные угрозы;
- угрозы при определенных условиях эксплуатации.

В первую часть входят угрозы, представляющие опасность для эксплуатируемых и создаваемых информационных систем (ИС). Их наличие определяется самим фактом создания ИС, являющейся по сути программно-аппаратной системой. Вторая же категория угроз зависит от условий, в которых эксплуатируется ИС или же для эксплуатации в которых она проектируется.

В свою очередь постоянные угрозы подразделяются на следующие группы:

- угрозы BIOS (УБИ 4, 5, 18, 24, 35, 45, 53, 87, 123, 144);
- угрозы объектам файловой системы и носителям информации (УБИ 67, 71, 88, 91, 156, 179);
- угрозы технических отказов по различным причинам (УБИ 51, 61, 114, 140, 180, 182, 166, 211);
- угрозы вредоносного программного обеспечения (УБИ 22, 27, 115, 170, 189, 208);
- угрозы средствам защиты информации (УБИ 185, 187, 214);
- угрозы несанкционированного доступа (УБИ 3, 7, 8, 12, 15, 23, 25, 28, 30, 31, 33, 34, 37, 49, 63, 68, 74, 86, 89, 90, 93, 95, 100, 102, 109, 117, 118, 121, 122, 124, 143, 149, 152, 155, 158, 162, 178, 205, 209, 212).

Угрозы при определенных условиях эксплуатации подразделяются на группы:

- угрозы при использовании виртуализации (УБИ 10, 44, 46, 48, 58, 59, 73, 75, 76, 77, 78, 79, 80, 84, 85, 108, 119, 120);

- угрозы при использовании внешних облачных технологий (УБИ 20, 21, 40, 43, 52, 54, 55, 56, 64, 65, 66, 70, 96, 101, 134, 135, 137, 138, 141, 142, 164);

- угрозы при наличии подключения к Интернет или иным сетям (УБИ 6, 16, 19, 17, 41, 42, 62, 92, 98, 99, 103, 104, 111, 116, 127, 128, 130, 131, 132, 145, 151, 153, 159, 167, 168, 171, 172, 173, 174, 175, 176, 181, 186, 188, 190, 193, 195, 197, 198, 201, 204, 215, 213, 217);

- угрозы при использовании Wi-Fi (УБИ 125, 126, 133, 11, 83);

- угрозы при использовании мобильных устройств (УБИ 184, 194, 196, 199, 200, 202, 216);

- угрозы при использовании грид–систем (УБИ 1, 2, 81, 110, 147, 47);

-угрозы при использовании систем больших данных и суперкомпьютеров (УБИ 29, 38, 50, 57, 60, 82, 97, 105, 106, 136, 146, 148, 161);

- угрозы для промышленных систем (УБИ 94, 107, 112, 183, 206, 207);

- угрозы, актуальные при обновлении программного обеспечения BIOS и микропрограммного обеспечения используемого оборудования (УБИ 9, 13, 32, 39, 72, 129, 150, 154, 210);

- угрозы при возможном физическом доступе посторонних лиц (УБИ 26, 69, 113, 157, 160, 139, 203);

- угрозы при использовании несертифицированного программного обеспечения (УБИ 165, 177, 191, 192, 36, 163, 169).

Такое разделение позволяет упростить определение угроз и, как следствие, проектировать систему защиты. Так, если в создаваемой информационной системе не планируется использование Wi-Fi и внешней виртуализации, то УБИ, связанные с ними, определяются как неактуальные.

Оставшиеся угрозы далее оцениваются на предмет их актуальности по методике, установленной регулятором [5].

Заключение.

По результатам проведенного исследования установлено, что при применении предложенного метода систематизации УБИ возможно определение

актуальных угроз безопасности информации для ИС. Предложенный метод позволяет упростить определение актуальных УБИ и может использоваться как дополнение к методам оценки угроз безопасности информации предоставляемым регулятором (ФСТЭК России).

Литература

1. Банк данных угроз безопасности информации [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/threat.
2. 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 2019. № 2(3). С. 64-68.
3. Борщева Н.В. Особенности построения модели угроз безопасности информации для государственных информационных систем //. Современные проблемы проектирования, производства и эксплуатации радиотехнических систем 2019. Сборник научных трудов Ульяновского государственного технического университета. С. 163-166.
4. Методический документ: Методика моделирования угроз безопасности информации. [Электронный ресурс]. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/149-proekty.
5. Методический документ: Методика оценки угроз безопасности информации. ФСТЭК России, 2021 год [Электронный ресурс].– Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g.

Literature

1. Databank of threats to information security [Electronic resource]. - Access mode: https://bdu.fstec.ru/threat.
2. Butin A.A., Ivanova E.V. Methodological aspects of building models of threats to information security for municipal authorities // Information technologies and

mathematical modeling in the management of complex systems 2019. No. 2 (3). P. 64-68.

3. Borshcheva N.V. Features of building a model of threats to information security for state information systems //. Modern problems of design, production and operation of radio engineering systems 2019. Collection of scientific papers of the Ulyanovsk state technical university. P. 163-166.
4. Methodological document: Methodology for modeling threats to information security. [Electronic resource]. - Access mode: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/149-proekty.
5. Methodical document: Methodology for assessing threats to information security. FSTEC of Russia, 2021 [Electronic resource]. - Access mode: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii 5-fevralya-2021-g.