УДК 004.62

Лебедев Дмитрий Валерьевич,
Магистрант,
Кафедра анализа систем и принятия решений,
Институт экономики и управления,
ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина,
г. Екатеринбург, Российская Федерация

АНАЛИЗ ДАННЫХ ОБ УГРОЗАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ФОРМИРОВАНИЯ КОМПЛЕКСНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация:
В управлении информационной безопасностью роль бизнеса является ключевой. Бизнес решает, как именно будет формироваться информационная безопасность в организации. И, как правило, компании не могут тратить большое количество денежных средств на финансирование отдела информационной безопасности и построения комплексных систем информационной безопасности (далее КСИБ).
В статье проанализированы угрозы безопасности информации из банка данных угроз Федеральной службы по техническому и экспортному контролю (далее ФСТЭК России). На основании данного анализа были определены наборы наиболее часто встречающихся способов реализации угроз безопасности информации, а также были приоритезированы меры по защите от реализации данных способов.

Ключевые слова:
Статистический анализ, Федеральная служба по техническому и экспортному контролю, банк данных угроз, моделирование, способы реализации атак, сценарии атак, меры защиты.

Введение

В бизнесе важно понимать для чего конкретно необходимо строить КСИБ. Одним из таких примеров может быть защита организации от действий злоумышленников, которые могут привести к потере денежных средств.

При этом существую определенные нормативные правовые акты, которые регламентируют деятельность, связанную с обеспечением информационной безопасности в организации. Примером таких нормативных правовых актов могут быть:

- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
- Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
- Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- Приказ ФСТЭК России от 11.02.2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
- Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 20.02.2020) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

ФСТЭК России осуществляет деятельность в организации государственной безопасности на уровне информационной безопасности. ФСТЭК России для определения потенциальных угроз для бизнеса предлагает такой инструмент как «Моделирование угроз безопасности информации». Подробное описание процесса моделирования угроз безопасности информации представлено в методическом документе ФСТЭК России «Методика оценки угроз безопасности информации».

Оценка угроз безопасности информации осуществляется для определения угроз безопасности информации, реализация которых возможна в информационных системах. Результатом оценки является выявление актуальных угроз безопасности информации [1]. Процесс оценки состоит из трех этапов:

1. Определение негативных последствий

В рамках данного этапа осуществляется анализ документации систем и сетей и иных исходных данных, а также определение негативных последствий от реализации угроз.

2. Определение объектов воздействия

Этап состоит из анализа исходных данных, инвентаризации систем и сетей и определения групп информационных ресурсов и компонентом систем и сетей.

3. Оценка возможности реализации угроз и их актуальности

Данный этап содержит определение источников атак, оценку способов реализации угроз и оценку актуальности угроз.

Актуальность угрозы определяется наличием сценариев их реализации. Сценарий реализации угрозы устанавливает последовательность возможных действий со стороны нарушителя информационной безопасности. Пример сценария реализации угроз безопасности информации представлен на рисунке 1.

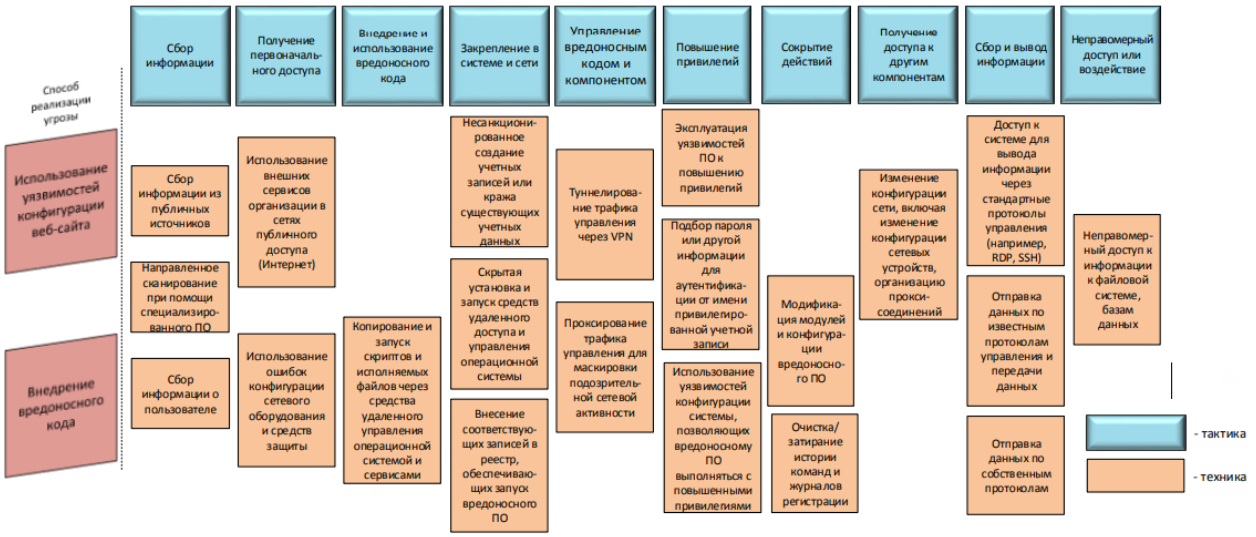

Рисунок 1 – Пример сценария реализации угрозы безопасности информации

Информация для каждого возможного действия нарушителя информационной безопасности представлена на портале банка данных угроз (далее БДУ) ФСТЭК России из состоит из информации [2]:

- Способ реализации
- Уровень возможностей нарушителя
- Возможные реализуемые угрозы
- Компоненты объектов воздействия
- Возможные меры защиты

На портале БДУ ФСТЭК России есть инструмент для автоматизированного моделирования угроз безопасности информации. Пример такого моделирования приведен в таблице 1.

Материалы и методы:

На основании анализа данных обо всех возможных угрозах с помощью инструмента для их автоматизированного моделирования возможно получить информацию о наиболее часто встречающихся способах реализации угроз и наиболее часто встречающихся мер защиты для нейтрализации угроз.

Для определения данной информации была получена отредактированная выборка по всем возможным угрозам. В таблице 2 приведен пример отредактированной выборки. Из отредактированной выборки были составлены таблицы А.1 и А.2 в приложении А с определенными часто встречающимися способами реализации угроз и мерами защиты.

Таблицы А.1 и А.2 были получены следующим образом:

1. Получение всех возможных угроз безопасности информации с портала БДУ ФСТЭК России.
2. Разделение информации по составу перечня сформированных угроз (объекты, компоненты, способы реализации, возможные меры защиты) по отдельным ячейкам в программном обеспечении Microsoft Excel.
3. Определение частоты появления каждого способа реализации угрозы безопасности информации и каждой меры по защите с помощью функции «СЧЕТЕСЛИ».
4. Ранжирование способов реализации угроз безопасности информации и мер по защите.

Результаты:

По результатам анализа данных об угрозах безопасности информации были сформированы таблицы А.1 и А.2, в которых представлены часто встречающиеся способы реализации угроз безопасности информации и меры по защите от них соответственно.

На рисунках 2 и 3 представлены топ 30 часто встречающихся угроз безопасности информации и мер по защите соответственно.

Таблица 1 – Пример моделирования угроз безопасности информации

Идентификатор	**Наименование**	**Описание**	**Объект воздействия**	**Компоненты**	**Способы реализации**	**Потенциал нарушителя**	**Меры защиты**
УБИ.10.2.3	Угроза распространения противоправной информации через компоненты сервера за счет использования недостатков архитектуры	Угроза заключается в изменении содержания или формы представления обрабатываемой в информационной системе информации (конфиденциальной, конфигурационной, аутентификационной и др.), нарушающем установленный в информационной системе порядок обработки информации. Например, искажение содержимого веб-сервера	О.2 Сервер	К.1.1.1 Прошивка (встроенная микропрограмма); К.1.3.1 Системные и сетевые службы	СП.3.1 Эксплуатация недостатков незащищенных протоколов передачи данных	В.1 Нарушитель, обладающий базовыми возможностями	ЗИС.19.1 Защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны; ЗИС.35.4 Отключение неиспользуемых сетевых протоколов компонентами инфраструктуры, хостовой операционной системы, вычислительной сети

Целью данной работы являлся анализ данных об угрозах безопасности информации, доступных на портале БДУ ФСТЭК России, для определения приоритетных действий по организации КСИБ.

Таблица 2 – Пример отредактированной выборки по всем возможным угрозам безопасности информации

Идентификатор	**Объект**	**Компонент 1**	**…**	**Компонент n**	**Способ реализации 1**	**…**	**Способ реализации n**	**Мера защиты 1**	**…**	**Мера защиты n**
УБИ.1.1.1	О.1	К.1.1.1	…	К.3.2.3	СП.1.1	…	СП.1.2	АУД.2	…	ОПС.2
УБИ.1.1.2	О.1	К.1.1.1	…	К.2.5.1	СП.2.1	…	СП.2.11	АУД.1	…	УПД.14
УБИ.1.1.7	О.1	К.1.1.1	…	К.3.1.2	СП.7.1	…	СП.7.7	АВЗ.1	…	СОВ.1
УБИ.1.2.10	О.2	К.1.1.1	…	К.3.1.2	СП.10.1	…	СП.10.7	ЗИС.27	-	-
УБИ.1.3.7	О.3	К.1.2.2	…	К.3.1.2	СП.7.1	…	СП.7.7	АВЗ.1	…	СОВ.1

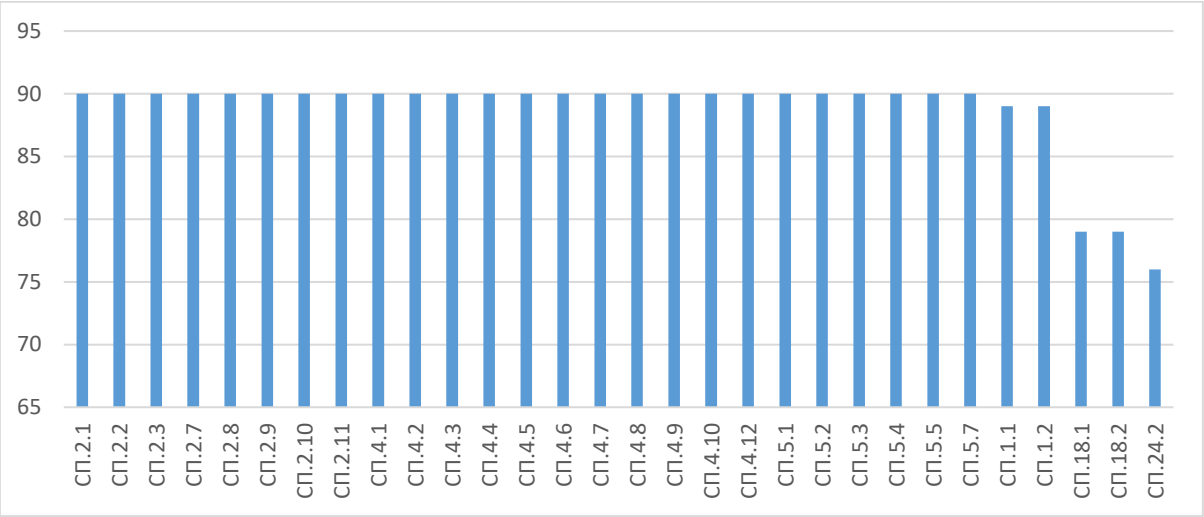

Рисунок 2 – Топ 30 часто встречающихся способов реализации угроз безопасности информации

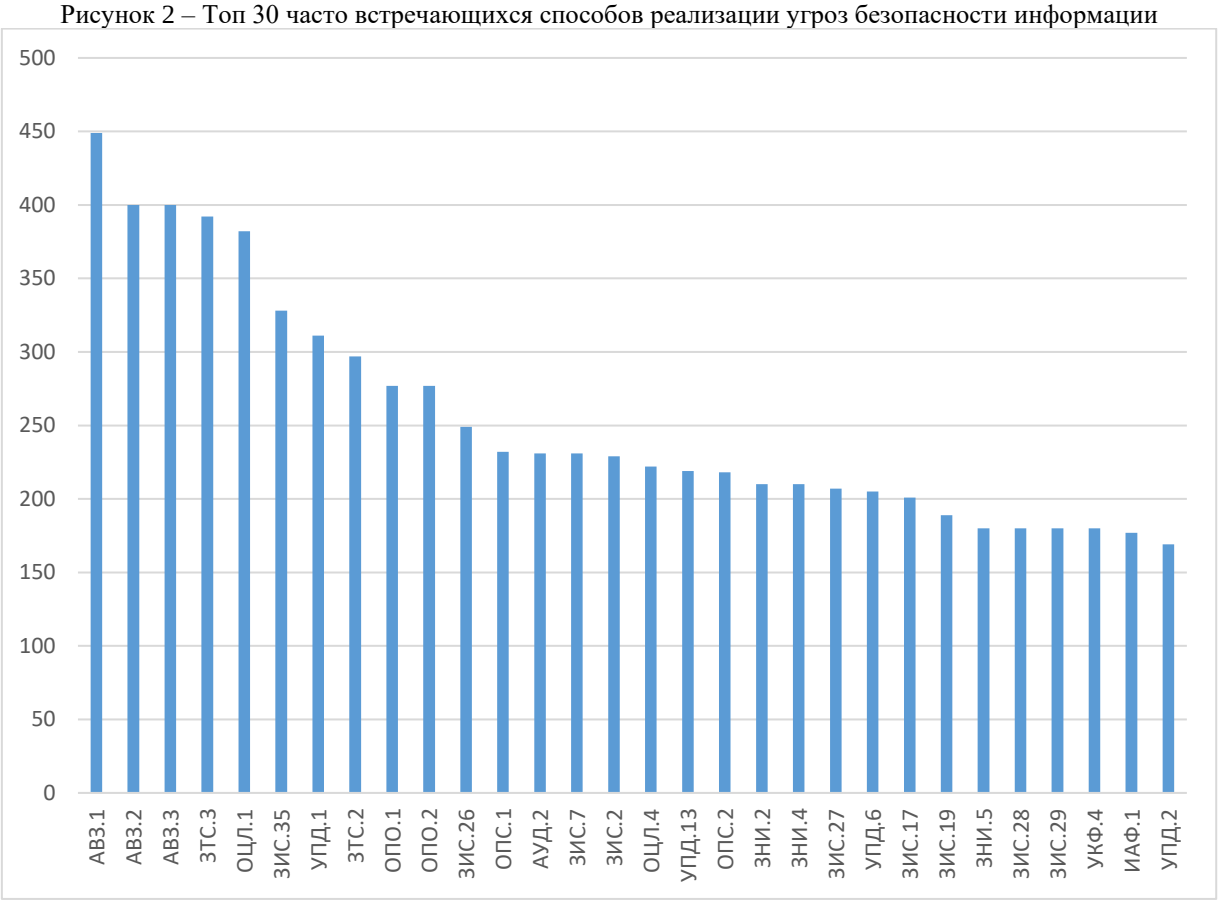

Рисунок 3 – Топ 30 часто встречающихся мер по защите от реализации угроз безопасности информации

Выводы:

Таким образом, в данной работе была проанализирована информация об угрозах безопасности информации с портала БДУ ФСТЭК России с целью определения наиболее часто встречающихся действиях злоумышленников. Также для данных действий были определены необходимые меры защиты для нейтрализации угроз безопасности информации.

Как видно из представленных результатов, большая часть способов реализации угроз безопасности информации, в большей степени является популярнее у злоумышленников, что позволяет сфокусировать ресурсы по организации КСИБ для нейтрализации приоритетных способов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Fstec.ru ФСТЭК России. Техническая защита информации. Документы. Методический документ. Методика оценки угроз безопасности информации. [Электронный ресурс]. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021, свободный. (дата обращения 06.03.2023)
2. Bdu.fstec.ru. Банк данных угроз безопасности информации. Угрозы. Новый раздел угроз. Формирование перечня угроз. [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/threat-section/shaper-threats, свободный. (дата обращения 06.03.2023)

Lebedev Dmitry Valerievich,
Master's student,
Department of Systems Analysis and Decision-Making,
Institute of Economics and Management,
Ural Federal University named after the First President of Russia B.N. Yeltsin,
Yekaterinburg, Russian Federation

ANALYSIS OF DATA ON INFORMATION SECURITY THREATS ANALYSIS FOR THE FORMATION OF A COMPREHENSIVE INFORMATION SECURITY SYSTEM

Abstract:
In information security management, the role of business is key. The business decides exactly how information security will be formed in the organization. And, as a rule, companies cannot spend a large amount of money on financing the information security department and building comprehensive information security systems.
The article analyzes the threats to the security of information from the threat database of the Federal Service for Technical and Export Control. Based on this analysis, sets of the most common ways of implementing information security threats were identified, and measures to protect against the implementation of these methods were prioritized.

Keywords:
Statistical analysis, Federal Service for Technical and Export Control, threat database, modeling, methods of implementing attacks, attack scenarios, protection measures.