МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ ПРИ ЗАЩИТЕ ОБЪЕКТОВ КРИТИЧЕСКИ ВАЖНОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Исмагилов Ильдар Рашидович

кандидат технических наук, доцент кафедры информатики и информационно управляющих систем КГЭУ.

Ахметшина Регина Ильдаровна

Студент 2 курса КГЭУ.

Гильманова Эллина Аделевна

Студент 2 курса КГЭУ.

Аннотация. Основной целью представленной статьи является изучение моделирования угроз безопасности при защите объектов критически важной информационной инфраструктуры. Автором приводится определение построения моделирования угроз безопасности, а также этапы данного моделирования.

Ключевые слова. Моделирование, безопасность, информация.

Отрасль энергетики России имеет ключевое значение для современного бизнеса, инфраструктуры, промышленности, а также повседневной и бытовой деятельности в жизни людей. Энергетические компании является основной мишенью для совершения кибератак со стороны других государств и иных киберпреступников, которые желают использовать этот сектор в своих политических или экономических целях.

Инновации и инновационная деятельность представляют из себя основный инструмент, обеспечивающий конкурентные преимущества энергетической отрасли. Помимо этого, на основе интеграции информационных технологий значительно повышается эффективность развития производства и экономической ситуации предприятия. Данный факт подтверждается множе-

ством экспертных оценок, которые указывают то, что треть экономического роста компании обеспечивается на основе инновационной деятельности. Разработка и интеграция инновационных технологий в энергетическом комплексе основана на направленных на это действиях, которые, в свою очередь, основаны на создании инновационной или же усовершенствовании уже существующей и функционирующей в энергетике техники.

Таким образом, современная сфера энергетики претерпела быструю цифровизацию, предоставив новые возможности киберпреступникам. Атаки спровоцированы высокой стоимостью активов и данных энергетической отрасли, а также сильно автоматизированными и слабо защищенными процессами и сетями. Хотя атаки в этом секторе зеркально отражают атаки в других отраслях, ставки значительно выше. Обеспечение и поддержание стабильной работы систем по обеспечению информационной безопасности является актуальным вопросом для корпораций, имеющих сложную, территориально-распределенную, многоуровневую структуру.

Моделирование угроз безопасности при защите объектов критически важной информационной инфраструктуры (КИИ) подразумевает описание свойств или характеристик угроз безопасности информации, а под угрозой безопасности - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации (т.е. базовых свойств информации, о которых мы уже говорили) [1].

Основная цель моделирования угроз КИИ заключается в нахождении всех условий и факторов, проводящих к нарушению безопасности информации и работы ИТ-систем. Модель угроз может строиться на основе следующего классического подхода: актуальная угроза информационной безопасности возникает при наличии источника угрозы (внешний/внутренний нарушитель или третьи силы), уязвимости актива, способа реализации угрозы, объекта воздействия и самого вредоносного воздействия [2].

Также необходимо отметить, что совсем недавно ФСТЭК России выпустил проект новой методики моделирования угроз безопасности информа-

ции, которую можно применять для моделирования угроз в критической информационной инфраструктуре. В соответствии с данной Методикой, угроза безопасности информации является актуальной, если существует источник угрозы, условия и сценарий для её реализации, а воздействие на активы приведет к негативным последствиям. В Методике сказано, что процесс моделирования угроз ИБ состоит из следующих этапов (рис. 1):

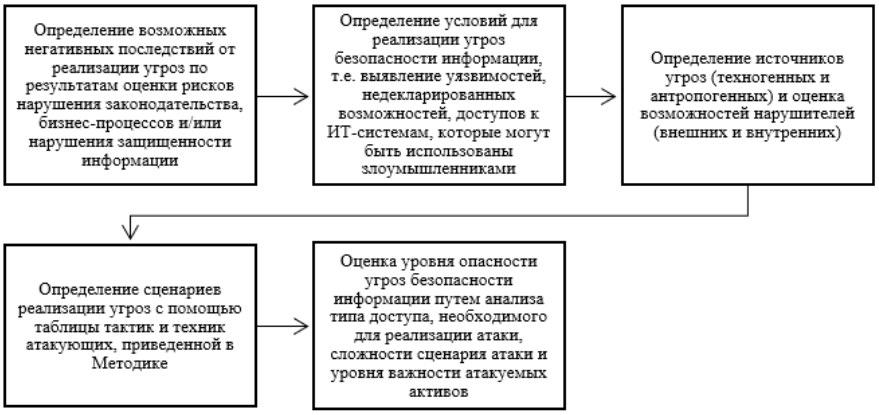

Рис. 1. Этапы моделирования угроз информационной безопасности

Также необходимо отметить, что разработка мер защиты информации значимого объекта критической информационной инфраструктуры и, как следствие, моделирование должно включать в себя анализ угроз безопасности и разработку модели угроз безопасности КИИ.

Анализ угроз включает выявление источников угроз, оценку возможностей нарушителей (т.е. создание модели нарушителя), анализ уязвимостей используемых систем, определение возможных способов реализации угроз и их последствий. Модель нарушителя строится на основе предположений о потенциале атакующих, т.е. о мере усилий, затрачиваемых нарушителем при реализации угроз безопасности информации в информационной системе (при этом потенциалы нарушителей можно условно разделить на высокий, средний и низкий).

Также необходимо отметить и аспект анализа уязвимостей, который производится посредством тестов на проникновение - пентестов (англ. PenTest, сокращение от Penetration Test). При проведении пентестов прове-

ряющие определяют слабые места инфраструктуры компании, выявляют уязвимости в системах защиты, проводят контролируемую эмуляцию настоящей хакерской атаки - в общем, наглядно показывают, что компания - заказчик этого тестирования может быть взломана. Далее заказчик получает рекомендации по устранению выявленных в ходе пентеста недочетов, и через какое-то время пентест повторяется.

Под построением модели угроз безопасности КИИ при защите КИИ подразумевается описание свойств или характеристик угроз безопасности информации, а под угрозой безопасности - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации (т.е. базовых свойств информации, о которых мы уже говорили). Целью моделирования угроз КИИ является нахождение всех условий и факторов, проводящих к нарушению безопасности информации и работы ИТ-систем [3].

Таким образом, выяснено, что моделирование угроз информационной безопасности при защите объектов критически важной информационной инфраструктуры имеет пять основных и необходимых этапов. При разработке средств по защите информации необходимо руководствоваться приведенными в статье данными, а также основываться на материалы новой методики моделирования угроз безопасности информации, разработанной ФСТЭК Российской Федерации. Необходимо отметить, что, основываясь на приведенной системе моделирования, можно разработать многоуровневую систему защиты информации, которая позволит более эффективно справляться с потенциальными угрозами, а также вычислять и производить операции, связанные с защитой информационных ресурсов более быстро относительно существующих на сегодняшний день программных решений.

Список литературы

1. Ковалев А. А., Балашов А. И. Международно-правовые аспекты политики кибербезопасности некоторых европейских стран бывшего советского блока // Вестник ПАГС. 2018.

2. Румянцев К. Е., Плёнкин А. П. Экспериментальные испытания телекоммуникационной сети с интегрированной системой квантового распределения ключей // Телекоммуникации. 2014.

3. Zagarskikh E.Yu., Zagarskikh Yu.A. The application of cybersecurity and the use of artificial intelligence in medicine // SAEC. 2019.