DOI 10.37882/2223-2982.2023.6-2.13

ОБОСНОВАНИЕ НЕОБХОДИМОСТИ РАЗРАБОТКИ ЭКСПЕРТНОЙ СИСТЕМЫ ОЦЕНКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

SUBSTANTIATION OF NECESSITY TO DEVELOP EXPERT SYSTEM FOR THREAT ASSESSMENT

A. Drugal
A. Tsaregorodtsev

Summary: An assessment of information security threats is necessary to develop an appropriate threat model. The new FSTEC information security threat assessment methodology has significantly increased the complexity of this process. This paper considers the features of the methodological document, notes the main factors that increase the complexity of threat assessment and substantiates the necessity to intellectualize this process. The result of the paper is a model of expert system usage for assessing information security threats.

Keywords: information security, threat assessment, expert system, threat model, threats to information security.

Другаль Артем Олегович
Финансовый университет при Правительстве Российской Федерации (Москва)
drugal-a@mail.ru
Царегородцев Анатолий Валерьевич
Финансовый университет при Правительстве Российской Федерации (Москва)
anvtsaregorodtsev@fa.ru

Аннотация. Оценка угроз безопасности информации необходима для разработки соответствующей модели угроз. Новая методика оценки угроз информационной безопасности ФСТЭК значительно увеличила трудоемкость данной задачи. В работе рассмотрены особенности методического документа, отмечены основные факторы, повышающие трудоемкость оценки угроз безопасности информации, обоснована необходимость интеллектуализации данного процесса. Результатом работы является модель применения экспертной системы для оценки угроз информационной безопасности.

Ключевые слова: информационная безопасность, оценка угроз, экспертная система, модель угроз, угрозы безопасности информации.

Введение

В современном мире системы защиты информации играют крайне важную роль в большинстве компаний и организаций, которые работают с различными видами данных. Утечка данных и кибератаки становятся все более частыми явлениями. Именно поэтому необходимо разрабатывать и применять эффективные системы защиты для того, чтобы обеспечивать безопасность данных.

Понимание угроз и рисков, связанных с использованием информационных технологий и хранением информации, является основой создания эффективных систем защиты. Модель угроз является одним из инструментов, которые помогают разработчикам систем защиты оценить угрозы и риски, связанные с их продуктами или услугами.

Модель угроз описывает потенциальные угрозы и атаки на систему, а также их последствия для информации и инфраструктуры. Она позволяет определить уязвимости в системе и потенциально опасные точки, которые могут стать объектом атак. Такая модель позволяет разработчикам понимать, какие меры по защите необходимо предпринять, для того чтобы устранить уязвимости и предотвратить нанесение ущерба.

Некоторые организации по каким-либо причинам могут не составлять модель угроз, а руководствоваться лучшими практиками по защите информации на рынке, среди конкурентов или следовать общим стандартам. Однако эти стандарты просто обеспечивают общее руководство по безопасности и не могут учитывать все нюансы конкретной системы. Общие стандарты почти всегда требуют дополнительной корректировки для конкретной системы [6].

Следует отметить, что процесс моделирования угроз должен быть строго систематизирован, иначе большое количество возможных атак может быть упущено. Для того чтобы скомпрометировать всю систему злоумышленнику достаточно найти лишь один вектор атаки. Поэтому разработчикам системы необходимо идентифицировать все возможные уязвимости системы. Анализ угроз следует проводить на самых ранних этапах проектирования системы. Хотя моделирование угроз системы на ранних этапах ее проектирования и в существующей системе требуют одинаковых затрат, устранение обнаруженных угроз в уже существующей системе становится затруднительной и дорогостоящей из-за наличия архитектурных ограничений [6].

Оценка угроз безопасности информации отличается практическим подходом. В настоящее время, из-за нехватки кадров, создание моделей угроз безопасности информации возлагается на множество сотрудников, работающих в области защиты информации. Во многих организациях задачи, связанные с защитой информации выполняют сотрудники, не являющиеся специалистами в области информационной безопасности.

Для тех специалистов, которые не обладают достаточной квалификацией в области информационной безопасности задача оценки угроз безопасности информации может быть не решаема. Поэтому организации вынуждены нанимать экспертов из сторонних организаций [3, 4], что приводит к повышению издержек организации на обеспечение безопасности информационной. Незнание всех тонкостей архитектуры и работы объекта информатизации может являться дополнительной сложностью для сторонних экспертов. Из-за этого задача оценки угроз информационной безопасности может быть выполнена не оптимально.

Анализ положений методики оценки угроз безопасности информации

Федеральная служба по техническому и экспортному контролю Российской Федерации 5 февраля 2021 года утвердила новый методический документ по оценке угроз информационной безопасности. Основной целью данного документа является структурирование процесса оценки и моделирования угроз безопасности информации [1]. Однако данная методика не является пошаговым руководством по построению модели угроз и, в связи с этим, специалист без соответствующей подготовки в области информационной безопасности не сможет решить задачу построения модели угроз для системы любого уровня сложности. Вместо этого, документ предоставляет лишь общий перечень основных этапов моделирования угроз и основных операций, выполнение которых не детализируется. Ответственность за выбор способов выполнения этих операций лежит на экспертах по безопасности информации [1].

Первым шагом при оценке угроз информационной безопасности с использованием нового методического документа ФСТЭК является определение негативных последствий, которые могут наступить при реализации угроз. В большинстве небольших организаций важной проблемой при обеспечении безопасности информационных систем является непонимание руководством необходимости обеспечения информационной безопасности. Зачастую руководители организации следуют лишь требованиям нормативных документов и стремятся выполнить эти требования с наименьшими затратами. Именно поэтому отделу информационной безопасности важно правильно сформулировать возможные негативные последствия, в том числе с описанием предполагаемых потерь в случае подобного инцидента. Это поможет оценить оправданность затрат на защиту информационной системы от предполагаемого инцидента.

Для решения этой проблемы методика предлагает определять те негативные последствия, которые понятны руководству организации. Для этого специалист по информационной безопасности может использовать нормативные документы организации, например, промышленные организации часто разрабатывают декларацию промышленной безопасности, в которой отражаются возможные последствия нарушения технологического процесса. Также во многих крупных организациях существуют специальные подразделения, которые проводят оценку и мониторинг рисков, связанных с деятельностью организации.

После определения возможных негативных последствий необходимо выявить воздействие на какие объекты информационной системы может привести к реализации угроз безопасности информации. Федеральная служба по техническому и экспортному контролю не детализирует то каким образом должны определяться объекты воздействия, оставляя это на усмотрения эксперта. Однако в методическом документе указано что необходимо использовать общий перечень угроз безопасности информации, опубликованный в банке данных угроз безопасности информации ФСТЭК России, а также другие общедоступные базы знаний с описанием угроз и векторов атак.

Также в методическом документе указано, что идентификация объектов воздействия не должна ограничиваться лишь компонентами системы, которыми управляет оператор. В случае применения на объекте информатизации облачных технологий, необходимо оценивать и возможность воздействия на элементы облачной инфраструктуры. Однако такую оценку должен проводить не оператор, а поставщик услуг облачных вычислений.

Исходя из того, что методика не определяет конкретного способа выявления возможных объектов воздействия, могут быть использованы различные подходы. Одним из возможных методов является применение сканера узлов сети. С его помощью можно провести инвентаризацию аппаратного и программного обеспечения, собрать параметры конфигурации операционных систем, служб, СУБД, прикладных систем и средств защиты информации, а также выявить известные уязвимости или ошибки конфигурации.

Следующим шагом после определения объектов воздействия является определение возможных источников угроз информационной безопасности. В качестве источников угроз в методике ФСТЭК рассматриваются только антропогенные источники.

В методике приводятся основные типы нарушителей: специальные службы иностранных государств, террористические организации, конкурирующие организации, бывшие сотрудники и другие. Важно отметить, что данный список не является исчерпывающим и может быть дополнен в случае необходимости. Также данный список

не стоит рассматривать как классификацию нарушителей, ведь бывший сотрудник может являться одновременно и элементом террористической организацией, работающей в интересах иностранного государства.

Данная методика предлагает 4 вида нарушителей, в зависимости от их возможностей по реализации угроз безопасности информации — от Н1 до Н4. Также данная методика подразделяет нарушителей на внешних и внутренних. Для каждого нарушителя необходимо определить цель его действий. В случае если мотив нарушителя соответствует одному или нескольким негативным последствиям, полученным при моделировании негативных последствий, такой нарушитель является актуальным для конкретной информационной системы.

Если в результате предыдущих шагов угроза признается возможной, необходимо оценить может ли нарушитель реализовать данную угрозу. Для этого необходимо рассмотреть сценарии нарушителя, при которых он из начального состояния мог бы получить возможности, необходимые для реализации угрозы.

Согласно нормативным документам ФСТЭК России, анализ угроз производится на стадии проектирования системы и регулярно на стадии эксплуатации системы. При анализе на стадии проектирования системы сценарий реализации угроз не может учитывать средства противодействия атакам и меры защиты, так как таких средств еще нет.

Угроза считается актуальной если существует хотя бы один сценарий ее реализации. Если угроза выявлена на этапе проектирования системы, то необходимо продумать усиление и дополнение мер защиты для нейтрализации угрозы. В случае выявления новой угрозы на этапе промышленной эксплуатации системы необходимо провести модернизацию системы защиты объекта информатизации.

Самым трудозатратным этапом в оценке актуальности угроз является оценка способов реализации угроз. Методика предлагает 10 основных тактик, которые в совокупности состоят из 145 техник, используемых для построения сценариев реализации угроз [1]. Предполагается, что для каждой угрозы эксперту необходимо проанализировать каждую из техник. Необходимо принять во внимание тот факт, что к данному этапу часть угроз уже будет исключена из рассмотрения, однако даже в этом случае на эксперта ложится задача анализа и оценки внушительного числа различных сценариев реализации угроз.

Кроме того, необходимо учитывать как скорость изменения количества актуальных угроз и уязвимостей, которые открывают новые сценарии реализации угроз, так и скорость модернизации используемых систем. Согласно базе данных CVE, в 2022 году было обнаружено и задекларировано 25227 уязвимостей. Причем количество новых уязвимостей растет на протяжении нескольких лет подряд. График количества обнаруженных уязвимостей представлен на рисунке 1.

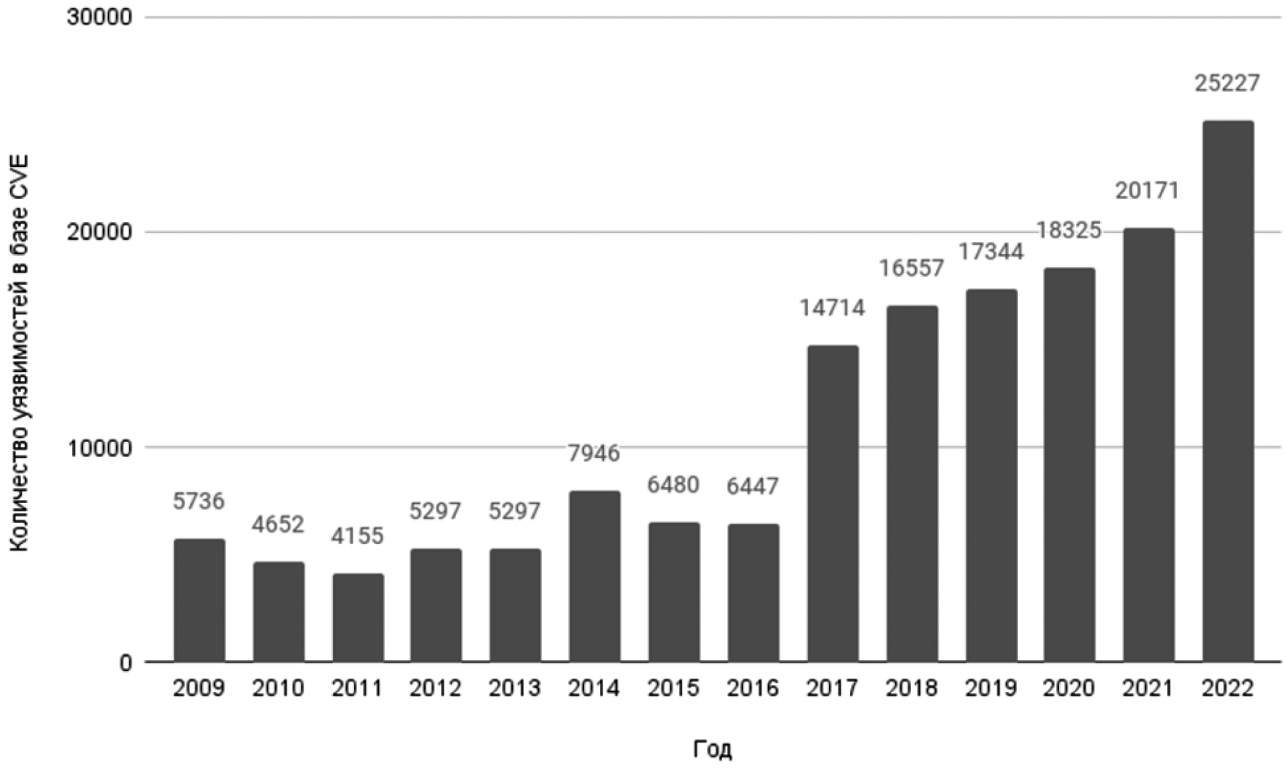

Рис. 1. Количество обнаруженных уязвимостей в базе данных CVE

Учитывая эти факторы методический документ предполагает проводить регулярные процедуры повторно оценки угроз для поддержания систем защиты информации в актуальном состоянии.

С увеличением количества систем и усложнении их архитектуры задача оценки угроз становится более сложной и трудозатраты, необходимые для решения этой задачи растут. Кроме того, для решения этой задачи методика предполагает привлечение специалистов из различных подразделений организации. Это необходимо в том числе для снижения влияния субъективного фактора при оценке угроз безопасности информации.

Кроме того, стоит отметить увеличение количества объектов информатизации, для которых применение данной методики является обязательным. Если ранее действующая методика оценки угроз применялась только для информационных систем персональных данных [2], то новая методика обязательно должна применяться для оценки угроз информационной безопасности в следующих системах:

- государственные и муниципальные информационные системы;
- информационные системы персональных данных;
- значимые объекты критической информационной инфраструктуры России;
- информационные системы управления производством, используемые оборонно-промышленным комплексом;
- автоматизированные системы управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды [1].

Таким образом, можно отметить следующие особенности новой методики оценки угроз информационной безопасности, которые повышают трудоемкость данной задачи:

- большое число необходимых для рассмотрения возможных сценариев реализации угроз;
- постоянный рост количества возможных угроз и уязвимостей информационных систем;
- необходимость регулярной актуализации результатов оценки угроз информационной безопасности;
- потребность формирования экспертной группы для оценки угроз;
- большое число различных объектов информатизации, для которых применение данной методики при оценке угроз информационной безопасности является обязательным.

В итоге появилась необходимость автоматизации процесса оценки угроз информационной безопасности. Благодаря внедрению автоматизированного комплекса можно добиться увеличения скорости получения результата, исключить риски, связанные с человеческим фактором, а также снизить затраты организации на обеспечение информационной безопасности.

Обоснование выбора средства автоматизации процесса оценки угроз информационной безопасности

В качестве средства для автоматизации процесса оценки угроз информационной безопасности выбрана экспертная система. Экспертные системы используются во многих областях, таких как медицина, финансы, юриспруденция, техническое обслуживание и другие.

Выбор данного метода обусловлен следующими особенностями экспертных систем. Во-первых, экспертные системы, в отличие от методов машинного обучения, предоставляют пользователю возможность запросить дополнительное объяснение вывода результата, что является полезным инструментом при анализе ошибочных или неожиданных результатов. Это позволяет удостовериться в правильности вывода системы, а также понять ее решения. Такой подход помогает пользователям делать более обоснованные и точные выводы, основываясь на более детальном анализе и понимании данных, и, в конечном счете, может привести к лучшим результатам и более эффективной работе. Такая возможность важна для оценки угроз информационной безопасности, так как из-за недостаточных мер обеспечения информационной безопасности организация может понести большие финансовые, репутационные и иные убытки. Кроме того, объяснение вывода результата может помочь в обучении новых пользователей экспертных систем.

Во-вторых, преимуществом использования экспертных систем является идемпотентность. При одних и тех же входных данных система вернет одинаковый результат вне зависимости от внешних воздействий.

Однако, экспертные системы могут оказаться неполными или ошибочными из-за ограниченности базы знаний или принятых правил. В таких случаях необходимо проводить дополнительную проверку и корректировку системы. Несмотря на это, затраты на актуализацию базы знаний значительно ниже затрат на проведение полной оценки угроз информационной безопасности.

Модель применения экспертной системы для оценки угроз информационной безопасности

Согласно новому методическому документу оценки угроз безопасности информации угроза безопасности информации является актуальной тогда и только тогда, когда существуют: способ реализации угрозы, предпо-

лагаемый нарушитель (источник) угрозы, объект, на который осуществляется воздействие, а также реализация данной угрозы может привести к реальным негативным последствиям. Данное условие можно выразить с помощью логического предиката:

$$A_i = У_i \wedge O_i \wedge H_i \wedge C_i \quad (1)$$

где i — индекс одной из угроз в базе данных угроз ФСТЭК России, A_i — актуальность i-й угрозы, $У_i$ — негативные последствия от реализации i-й угрозы, O_i — объект воздействия i-й угрозы, H_i — нарушитель, C_i — способ реализации i-й угрозы.

Для нарушителя при этом необходимо определить уровень его возможностей с помощью определения базового потенциала. Лучше всего при оценке базового потенциала нарушителя воспользоваться методом экспертных оценок. Для этого каждому эксперту необходимо оценить по 10 балльной шкале общие технические знания нарушителя, осведомленность об архитектуре системы и особенностях эксплуатации, уровень мотивации, уровень оснащенности. Оценка базового потенциала нарушителя рассчитывается по формуле:

$$P_j = \sum_{i=1}^{n}\left[w_i \cdot \left(TK_{j,i} + SK_{j,i} + M_{j,i} + E_{j,i} \right) \right] \quad (2)$$

где P_j — оценка базового потенциала j-го нарушителя, w_i — весовой коэффициент i-го эксперта, $TK_{j,i}$ — оценка уровня общих технических знаний j-го нарушителя i-м экспертом, $SK_{j,i}$ — оценка уровня осведомленности j-го нарушителя об архитектуре системы и особенностях эксплуатации i-м экспертом, $M_{j,i}$ — оценка уровня мотивации j-го нарушителя i-м экспертом, $E_{j,i}$ — оценка уровня оснащенности j-го нарушителя i-м экспертом.

Вес эксперта при этом может быть рассчитан по формуле:

$$w_i = \frac{K_i}{\sum_{j=1}^{n} K_j} \quad (3)$$

где n — количество экспертов, K_i — количество баллов, полученное i-м экспертом при его оценке, w_i — вес i-го эксперта.

Оценка экспертов при этом может осуществляться с помощью различных методик, например, с помощью тестирования.

Таким образом, возможности нарушителя по реализации угроз безопасности информации в зависимости от оценки базового потенциала:

$$B = \begin{cases} \text{высокие, при } P \geq 8, \\ \text{средние, при } 5 \leq P < 8, \\ \text{базовые повышенные, при } 3 \leq P < 5, \\ \text{базовые, при } P < 3. \end{cases}$$

Таким образом, база знаний экспертной системы должна содержать:

1. Информацию о всех возможных угрозах и уязвимостях из БДУ ФСТЭК России [5], а также иметь возможность оперативно их обновлять
2. Информацию о всех возможных объектах воздействия для каждого из уровней (сетевой, системный, прикладной, уровень пользователей)
3. Информацию о возможных нарушителях, их целях и уровнях их возможностей
4. Информацию о всех возможных способах реализациях угроз безопасности информации, а также основных мерах противодействия каждому из способов

Перед использованием системы пользователю необходимо провести инвентаризацию на объекте информатизации.

Для определения возможных негативных последствий пользователь должен для каждой угрозы указать перечень негативных последствий, которые могут возникнуть при реализации данной угрозы информационной безопасности. Если при реализации угрозы на данном объекте информатизации нет негативных последствий, то такая угроза не является актуальной.

Для определения списка объектов воздействия пользователю для каждого из уровней (сетевой, системный, прикладной, уровень пользователей) должен предлагаться исчерпывающий список с возможностью выбора актуальных программных и аппаратных средств, используемых на объекте информатизации.

В методическом документе представлены основные виды нарушителей, а также указаны основные цели, которые данные нарушители преследуют. Для каждого объекта информатизации с учетом его специфики должны быть указаны все актуальные нарушители и актуальные цели нарушителей. Если цель, преследуемая конкретным нарушителем, не может быть достигнута при реализации угроз на данном объекте информатизации, то такой нарушитель не является актуальным для рассматриваемого объекта.

В методическом документе представлены основные способы реализации угроз информации. Для каждого способа кроме уязвимостей, содержащихся в БДУ, должны быть представлены меры противодействия. Для этого пользователь должен выбрать имеющиеся меры про-

тиводействия для каждого из способа реализации угроз. При наличии меры или комплекса мер противодействия такой способ реализации угрозы не является актуальным для рассматриваемого объекта информатизации.

В результате работы экспертной системы пользователь должен получить перечень актуальных угроз для объекта информатизации, нарушителей, действия которых могут привести к реализации угроз, объектов воздействия, а также негативных последствий.

Заключение

В данной работе проведен анализ основных положений методики оценки угроз информационной безопасности ФСТЭК России, выделены основные факторы, увеличивающие трудозатраты при оценке угроз с применением новой методики, обоснована необходимость автоматизации процесса оценки угроз, представлена математическая модель работы экспертной системы оценки угроз информационной безопасности, предложена методика оценки возможностей нарушителя с помощью метода экспертных оценок.

По предварительным оценкам, использование экспертной системы при оценке угроз информационной безопасности будет требовать меньше трудозатрат по сравнению с ручным анализом через 3 года после начала разработки.

Подводя итог, можно отметить, что разработка экспертной системы оценки угроз информационной безопасности позволит сократить финансовые издержки предприятия, связанные с определением списка актуальных угроз для объекта информатизации, ускорить сам процесс моделирования угроз, а также избежать ошибок, полученных в результате человеческого фактора.

ЛИТЕРАТУРА

1. Методический документ ФСТЭК России «Методика оценки угроз безопасности информации». Утвержден ФСТЭК России 5 февраля 2021 года.
2. Методический документ ФСТЭК России от 14.02.2008 «Методика определения актуальности угроз безопасности персональных данных при их обработке в информационных системах персональных данных»
3. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
4. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при обработке в информационных системах персональных данных».
5. БДУ — Угрозы [Электронный ресурс]. — URL: https://bdu.fstec.ru/threats (Дата обращения 15.04.2023). Загл. с экр. Яз. рус.
6. Myagmar, Suvda & Lee, Adam & Yurcik, William. (2005). Threat Modeling as a Basis for Security Requirements.

Журнал «Современная наука: актуальные проблемы теории и практики»