УДК 004.056/053

С.П. Серёдкин[1]

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

МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ОСНОВЕ БАНКА УГРОЗ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ РОССИИ

Аннотация. В предлагаемой статье описан механизм моделирования угроз безопасности информации на основе данных банка угроз ФСТЭК. Описывается механизм реализации требований по моделированию угроз безопасности информации, на основе Новой методики, принятой ФСТЭК 05.02.2021. Предложен подход к построению модели угроз безопасности информации, учитывающей современные требования регуляторов, которые базируются на БДУ ФСТЭК. Подчеркнута важная роль использования данных базы угроз ФСТЭК для построения актуальной модели угроз с применением техник и тактик потенциального нарушителя. Акцентировано особое внимание на обязательном применении данной методики при моделировании актуальных угроз безопасности информации в государственных информационных системах, значимых объектах критической информационной инфраструктуры, информационных системах оборонно-промышленного комплекса, а также в информационных системах персональных данных. Проанализированы современные подходы и возможности интернет ресурсов для поиска угроз и анализа уязвимостей актуальных в настоящее время их преимущества и недостатки. Даны практические рекомендации для применения интернет ресурса ФСТЭК студентами высших учебных заведений и специалистами по защите информации учреждений и организаций при моделировании угроз безопасности информации.

Ключевые слова: Угрозы информационной безопасности, уязвимости информационных систем, Федеральная служба по техническому и экспортному контролю (ФСТЭК), банк данных угроз (БДУ), информационная безопасность (ИБ), потенциальный нарушитель, модель угроз безопасности информации, негативные последствия, модель нарушителя, государственные информационные системы (ГИС).

S.P. Seryodkin[1]

[1]Irkutsk State Transport University, Irkutsk, Russian Federation

MODELING OF INFORMATION SECURITY THREATS BASED ON THE THREAT BANK OF THE FEDERAL SERVICE FOR TECHNICAL AND EXPORT CONTROL OF RUSSIA

Abstract. In the proposed article we describe a mechanism of modeling information security threats which based on data of the FSTEC security threat bank. The mechanism of implementation of requirements for modeling information security threats is described, based on a new methodology adopted by FSTEC 05.02.2021. An approach to build a model of information security threats taking into account the modern requirements of regulators, which are based on the FSTEC database is proposed. The important role of using the FSTEC threat database data to build an up-to-date threat model using techniques and tactics of a potential violator is emphasized. Special attention is paid to the mandatory application of this technique in modeling current threats to information security in state information systems, significant objects of critical information infrastructure, information systems of the military-industrial complex, as well as in personal data information systems. Modern approaches and capabilities of Internet resources for threat search and vulnerability analysis are analyzed, their advantages and disadvantages are currently relevant. Practical recommendations are given for the use of the FSTEC Internet resource by students of higher educational institutions and information security specialists of institutions and organizations in modeling information security threats.

Keywords: Threats to information security, vulnerabilities of information systems, threat data bank (TDB), potential violator, information security threat model, negative consequences, violator model, state information systems (SIS), Federal Service for Technical and Export Control (FSTEC), Threat Data Bank (DBU), information security (IS), potential violator, state information systems (GIS).

Введение. В современном информационном пространстве отмечается повышенное влияние глобальных информационных технологий на основные сферы деятельности общества. Анализ текущего положения показывает, что процесс создания средств зашиты информации, отстает от темпов развития компьютерных технологий. Наиболее актуальными являются задачи по выявлению, анализу и классификации существующих механизмов

осуществления угроз информационной безопасности, Обеспечение высокого уровня организационных и технических мероприятий, направленных на защиту информации должны строится на системно методическом подходе к данной проблеме.

Наиболее важным этапом создания и модернизации системы защиты информации на предприятии является разработка модели угроз. Построение модели угроз информационной безопасности позволяет определить существующие угрозы, разработать эффективные меры противодействия, тем самым довести уровень защиты информации до требуемого.

Нормативно правовая база по моделированию угроз ИБ в 2021 году пополнилась важным, на наш взгляд документом: «Методический документ. Методика оценки угроз безопасности информации» Утвержден ФСТЭК России 5 февраля 2021 г. [15].

В связи с вводом в действие настоящего методического документа не применяются для оценки угроз безопасности информации:

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ФСТЭК России, 2008 г.);

Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (ФСТЭК России, 2007г.).

По сути, государством предложен универсальный механизм построения модели угроз. Основываясь на банк данных актуальных угроз ФСТЭК и Методику оценки угроз безопасности информации, предприятия и учреждения имеют возможность реализовать необходимые меры по защите информации, тем самым обеспечивая условия для реализации необходимых мер национальной и международной безопасности в противодействие угрозам [15].

Новое в Методике оценки угроз

Ранее для определения потенциальных угроз безопасности информации использовали одну из следующих методик:

- методику определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (2008 г.);
- методику определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (2007 г.) [11]. Данные документы в 2021 году утратили свою актуальность, т.к. были узкоспециализированными и ограничивали область применения на различных объектах информатизации.

Методика оценки угроз безопасности информации, утверждённая 05.02.2021. ФСТЭК России применяется на следующих типах объектов [2]:

- информационные системы (ИС);
- автоматизированные системы управления;
- информационно-телекоммуникационные сети;
- информационно-телекоммуникационные инфраструктуры центров обработки данных;
- облачные инфраструктуры.

А также является обязательной для применяется в следующих областях:

- информационные системы персональных данных;
- информационные системы управления производством, используемые организациями оборонно-промышленного комплекса;
- муниципальные и государственные ИС;
- значимые объекты критической информационной инфраструктуры РФ;
- критически важные, потенциально опасные объекты с автоматизированными системами управления производственными и технологическими процессами.

Моделирование угроз необходимо для решения двух задач:

- на стадии создания информационной систем и информационно-телекоммуникационных сетей, для определения предъявляемых к ним требований безопасности информации;

- на стадии их эксплуатации, для выявления новых актуальных угроз и принятия решения о необходимости модернизировать систему защиты информации.

В данной методике изменён сам порядок оценки угроз информации и состоит из этапов:

- определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;
- определение возможных объектов воздействия угроз безопасности информации;
- оценке возможности реализации (возникновения) угроз безопасности информации и определение их актуальности [2].

Схема проведения оценки угроз безопасности, представленная на рис. 1.

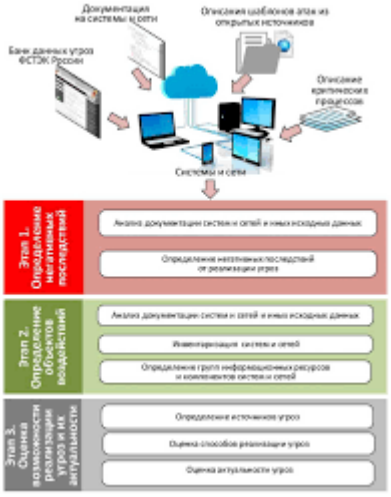

Рис. 1: Общая схема проведения оценки угроз безопасности информации

Так же в документе изменён механизм построения модели угроз, а именно отправной точкой к построению модели угроз безопасности информации. является этап определения вероятности возникновения негативных последствий, рис.2. Важно то что, взаимосвязь базы данных уязвимостей программного обеспечения и программно-аппаратных средств с перечнем актуальных угроз информационной безопасности это главное, что ложится в основу моделирования угроз.

Рис. 2: Этапы моделирования угроз безопасности информации

Этапы построения модели угроз:

1. Определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации; т.е необходимо определить те негативные последствия, которые могут причинить серьёзный ущерб. Для формального соответствия методике достаточно определять негативные последствия на том уровне абстракции, который

используется (см. Приложение 4 методического документа «Виды рисков (ущерба) и типовые негативные последствия от реализации угроз безопасности информации») [2]. На практике целесообразно изначально составить максимально подробный перечень таких последствий, и в дальнейшем, при анализе угроз для конкретной информационной системы, выбрать из них те, которые могут быть актуальными для этой системы, рис.3.

Рис. 3: Определение негативных последствий

2. Инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации; На данном этапе необходимо определить, воздействие на какие именно объекты может привести к наступлению негативных последствий, рис.4. Методический документ не детализирует, как именно должны определяться объекты воздействия, оставляя это на усмотрение эксперта, проводящего анализ уязвимостей. При этом:

- необходимо воспользоваться информацией из банка угроз безопасности информации (БДУ) ФСТЭК России;

- кроме этого требуется использовать низкоуровневые описания возможных способов воздействия, описанных в базах знаний CAPEC и Att&CK, а также в базах знаний типовых атак на веб-приложения WASC и OWASP. Один из приемов, дающих хорошие практические результаты, основан на пошаговом анализе детализации бизнес-процессов. В результате чего формируется перечень компонентов информационных систем, которые могут представлять интерес для нарушителя, стремящегося добиться наступления моделируемого негативного последствия.

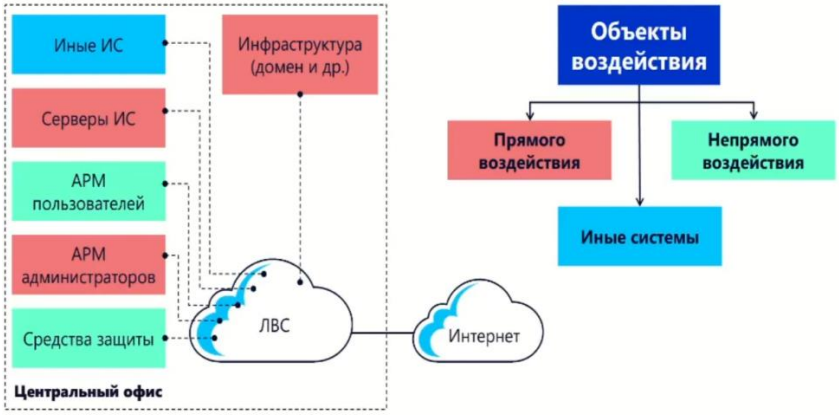

Рис. 4: Определение объектов воздействия

3. Определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации.

Основная задача, которая решается определением видов нарушителя – сформулировать цель действий нарушителя и решить, признается ли нарушитель данного вида актуальным для

информационной системы, рис.5. В случае, если одно или несколько рассматриваемых в процессе моделирования негативных последствий, соответствуют целям, определенным для данного вида нарушителей (см. Приложение 6 методического документа «Возможные цели реализации угроз безопасности информации нарушителями»). Таким образом, методика указывает прямое соответствие между негативными последствиями, целями нарушителей различных видов и их возможностями.

Рис. 5: Моделирование возможных нарушителей ИБ

4. Оценка способов реализации (возникновения) угроз безопасности информации; После того, как определены объекты воздействия и источники угроз, необходимо оценить, может ли рассматриваемый источник угроз реализовать угрозу, приводящую к негативным последствиям.

5. Оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;

Угрозой признается возможной, если определяется нарушитель, целям которого соответствуют негативные последствия реализации угрозы, и возможности которого позволяют выполнить соответствующее воздействие.

6. Оценка сценариев реализации угроз безопасности информации в системах и сетях, рис.6.

Если угроза признается возможной, остается оценить может ли выбранный нарушитель практически реализовать угрозу, рассмотрев возможные сценарии реализации угрозы – последовательности тактик и техник действий нарушителя необходимые для реализации угрозы. Угроза признается актуальной, если есть хотя бы один сценарий ее реализации. На стадии создания информационной системы актуальность угрозы означает необходимость усиления и дополнения базового набора мер защиты с тем, чтобы нейтрализовать угрозу. На стадии эксплуатации актуальность угрозы означает необходимость модернизации системы защиты, направленную на усиление и дополнение уже реализованных мер защиты.

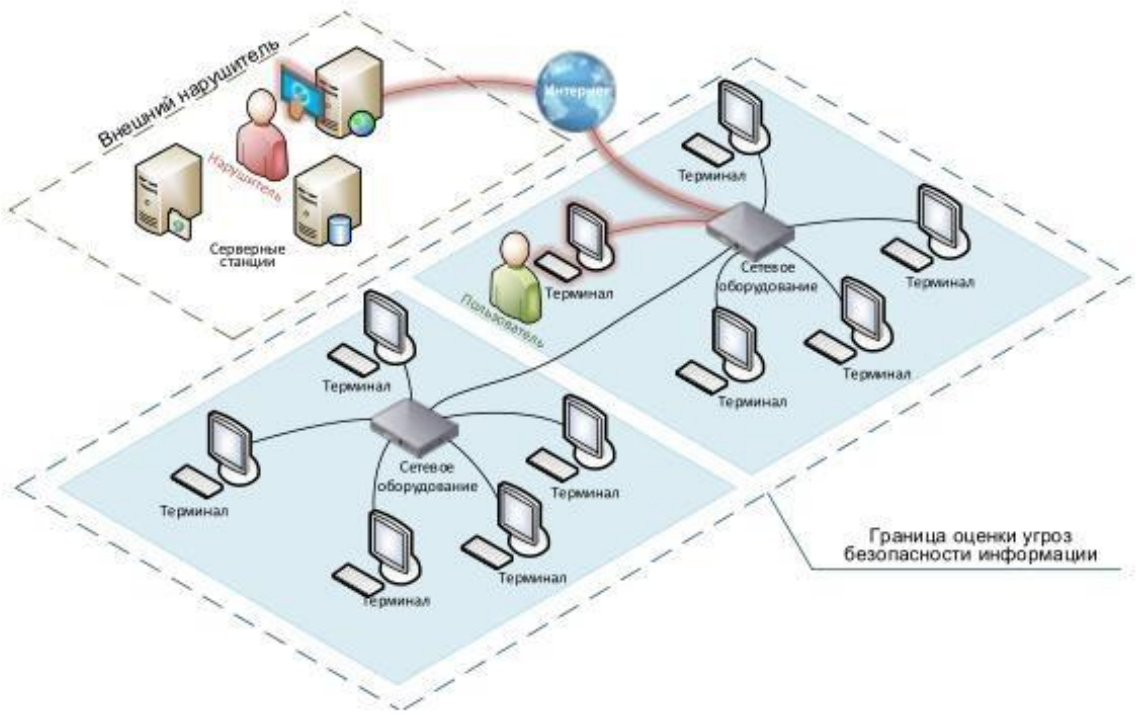

Рис. 6: Пример сценариев реализации угроз безопасности информации

В методике используется оценка угроз безопасности с применением сценариев действий нарушителей и не включает в себя ряд факторов, которые не зависят от человека:

- угрозы безопасности, связанных с природными явлениями и стихийными бедствиями;
- угрозы безопасности криптографических средств защиты;
- угрозы безопасности, связанных с техническими каналами утечки данных.

В свою очередь субъекты информационных систем в праве включать техногенные угрозы в модель угроз ИБ.

Практическое использование БДУ ФСТЭК при моделировании угроз

По данным исследования компании «Positive Technologies» в 2021г. промышленные предприятия подвергались атакам. Основными методами атак остаются фишинговые рассылки (56%) и хакинг (35%), причем доля последнего стабильно растет в течение нескольких лет. Успешность применения этого метода злоумышленниками свидетельствует о низком уровне защищенности промышленных организаций, наличии большого числа уязвимостей и недостатков защиты, как на периметре сети, так и во внутренней инфраструктуре [3].

Очевидно, что в такой ситуации специалисты по ИБ, ответственные за безопасное функционирование промышленных автоматизированных систем, остро нуждаются в наличии эффективной информационно-аналитической поддержки, с помощью которой они могли бы не только своевременно реагировать на ту или иную реальную атаку, но и прогнозировать (предупреждать) появление такого рода атак.

Сегодня в государственных информационных системах (ГИС), является обязательным использование БДУ ФСТЭК при построении модели угроз.

Целью создания и ведения банка угроз явилось – создание единой системы учета, хранения и предоставления информации об угрозах безопасности и уязвимостях.

Задачи, решаемые при ведении банка данных угроз:

1. Выявления, анализ и проверка сведений об уязвимостях;
2. Внесение сведений об уязвимостях и угрозах;

3. Поддержание информации об уязвимостях в актуальном состоянии;
4. Предоставление доступа к хранимой информации;
5. Своевременное информирование о новых уязвимостях и организация работ по их устранению.

Специалисту по защите информации необходимо ознакомиться с перечнем актуальных нормативных актов и документов ФСТЭК, банками данных угроз и уязвимостей последней версии, рис.7.

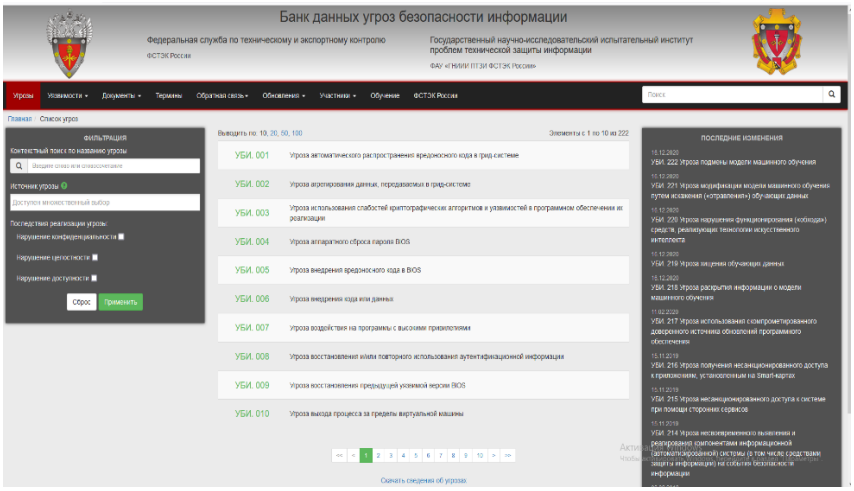

Рис. 7: База данных банка угроз безопасности ФСТЭК

Одним из важных аспектов исходных данных для оценки угроз безопасности информации является общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России который ведется ФСТЭК с 2015 г. и размещён в общем доступе по адресу: www.bdu.fstec.ru. Кроме того, дополнительно к этому для оценки УБИ рекомендуется использовать описание векторов атак, содержащихся в сторонних базах знаний, таких как CAPEC, ATT&CK, OWASP, STIX, WASC и др. [12]. По сути ФСТЭК России предоставил возможность специалистам по защите информации учреждений и организаций, воспользоваться актуальными данными, а не определять угрозы и уязвимости систем самостоятельно. Тем самым исключив не компетентный подход к данной процедуре. Работа с банком угроз и уязвимостей ФСТЭК это системная и результативная работа по построению эффективной системы защиты.

Для примера рассмотрим УБИ. 090 «Угроза несанкционированного создания учётной записи пользователя», рис.8. Данная угроза «заключается в возможности создания нарушителем в системе дополнительной учётной записи пользователя и её дальнейшего использования в собственных неправомерных целях (входа в систему с правами этой учётной записи и осуществления деструктивных действий по отношению к дискредитированной системе или из дискредитированной системы по отношению к другим системам). Данная угроза обусловлена недостатком механизмов разграничения доступа к защищаемой информации. Реализация данной угрозы возможна в случае наличия и прав на запуск специализированных программ для редактирования файлов, содержащих сведения о пользователях системы (при удалённом доступе) или штатных средств управления доступом из состава операционной системы (при локальном доступе) [15].

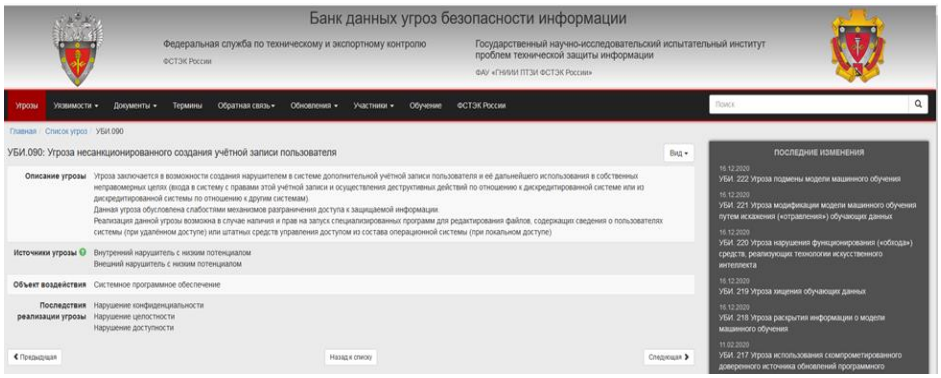

Рис. 8: УБИ. 090 Угроза несанкционированного создания учётной записи пользователя

Как в рамках существующих методик анализа угроз можно интерпретировать «последовательность неправомерных действий»? При наличии данной угрозы существует потенциальная возможность причинения ущерба организации путем компрометации информационного актива, т.е угроза безопасности информации (УБИ). УБИ представляет собой некую последовательность действий (и/или событий). Данная последовательность действий подразделяется на основные этапы - это Тактики. На каждом этапе злоумышленник выполняет определенный набор действий, используя определенные технические приемы для реализации атаки - это Техники. Сценарии реализации УБИ злоумышленником – это набор конкретных техник и тактик, количество которых может доходить до нескольких тысяч. Любая уязвимость порождает свои техники. Сценарий реализации УБИ злоумышленником, далее Модель — нарушителя- это последовательность конкретных Тактик и Техник, применяемых для реализации угрозы. Учитывая тот факт, что для реализации конкретной угрозы необходимо рассмотреть огромное количество сценариев применения техник и тактик, поэтому в базах знаний применяются типовые техники и тактики. Так как объектом воздействия является системное программное обеспечение, БДУ ФСТЭК позволяет найти актуальную уязвимость, используя типовое приложение [15].

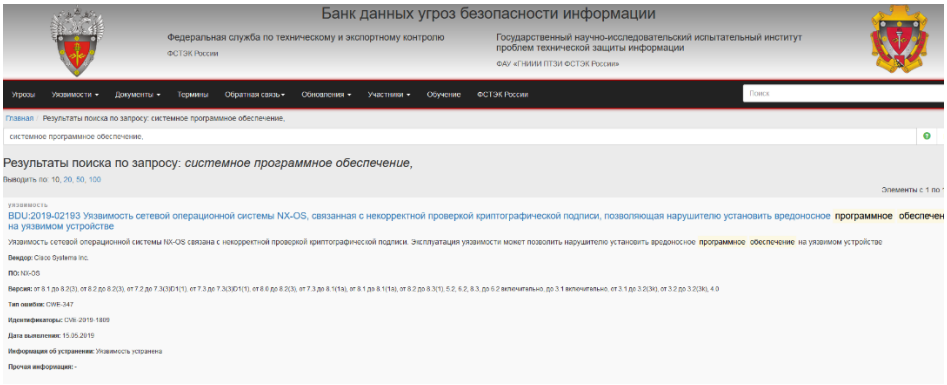

Рис. 9: BDU:2019-02193: Уязвимость сетевой операционной системы

Таким образом реализация УБИ. 090 (как и большинства умышленных антропогенных угроз), как правило, начинается с формирования у злоумышленника замысла и мотивации, далее осуществляется сбор информации о системе, проводится рекогносцировка, получив к ней первоначальный доступ тем или иным неправомерным способом, при необходимости проводится эскалацию привилегий, далее осуществляется поиск и получение доступа к защищаемой информации.

Это типовой сценарий реализации угрозы на тактическом уровне. На уровне техник для каждой из упомянутых тактик (этапов реализации угрозы) необходимо рассмотреть действия нарушителя. В условных цифрах для каждой из примерно 200 УБИ необходимо проанализировать по 10 типовых тактик для каждой и по 20 техник в рамках каждой тактики. Это даст порядка 40 000 типовых сценариев, из которых надо решить, какие применимы в

данной ситуации. Далее для применимых типовых Сценариев, необходимо разобрать их варианты, т.к. применяемые Техники могут различным образом комбинироваться в рамках одной Тактики. Это увеличит количество анализируемых Сценариев примерно до 400 000. Из приведенного примера видно, что данный объем работ реализовать очень трудоемко. Поэтому для перехода к реальным сценариям необходимо воспользоваться БДУ ФСТЭК, учитывая особенности конкретной ИС. Далее после оценки сценариев реализации угроз осуществляем поиск уязвимостей уязвимостей CVSS V2 БДУ ФСТЭК. Для этого воспользуемся калькулятор CVSS V2 «Справочные сведения об общей системе оценки уязвимости». Ресурс ФСТЭК – CVSS. Общая система оценки уязвимостей (Common Vulnerability Scoring System – CVSS) – это система, которая позволяет осуществлять сравнение уязвимостей программного обеспечения с точки зрения их опасности. Осуществляем запрос по УБИ.090 и получаем актуальные уязвимости для исследуемой ИС. BDU:2019-02193, рис.9,10. Уязвимость сетевой операционной системы NX-OS, связанная с некорректной проверкой криптографической подписи, позволяющая нарушителю установить вредоносное программное обеспечение на уязвимом устройстве.

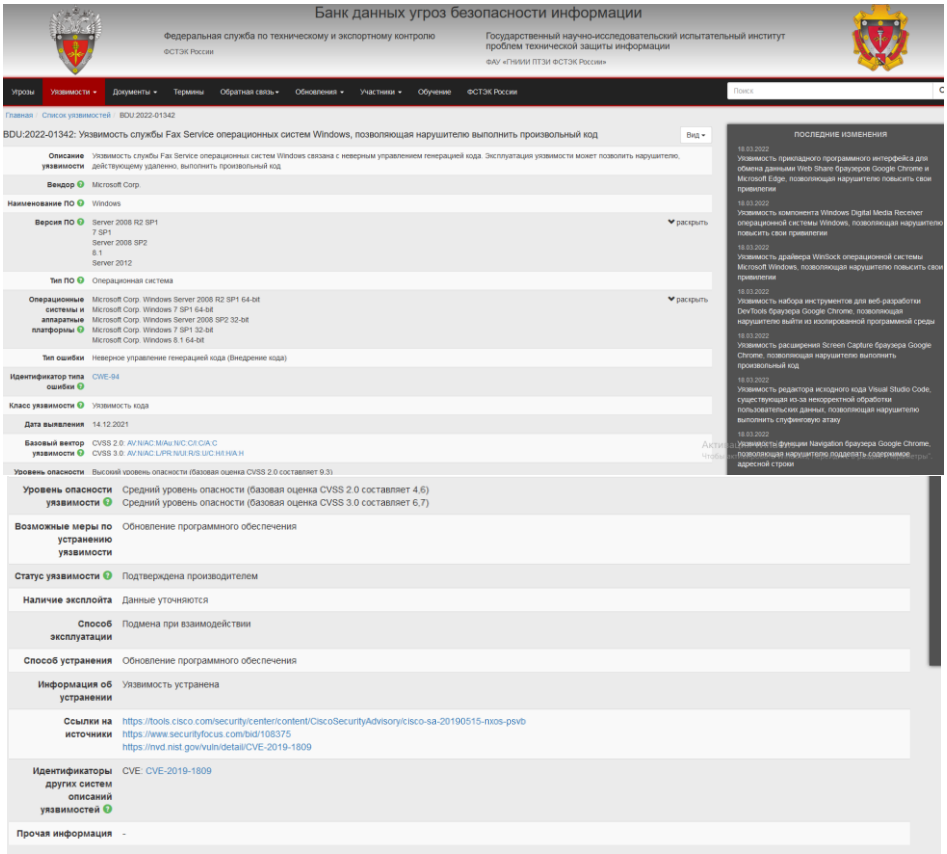

Рис. 10: Уязвимость BDU:2019-02193

Исходя из этого угроза УБИ. 090 «Угроза несанкционированного создания учётной записи пользователя» может быть реализована через уязвимость BDU:2019-02193: «Уязвимость сетевой операционной системы NX-OS», что в свою очередь может привести к негативным последствиям. Основные виды ущерба и возможные негативные последствия, к которым может привести нарушение конфиденциальности, целостности, доступности информации, приведены в таблице 6, в свою очередь степень возможного ущерба определяется экспертным методом в соответствии с таблицей 7 методического документа. Решение об актуальности данной угрозы безопасности информации для информационной системы с заданными структурно-функциональными характеристиками и условиями функционирования принимается в соответствии с таблицей 8 методики [2].

Таким образом, мы описали механизм моделирования угроз безопасности с применением БДУ ФСТЭК. В результате чего было установлено, существует ли возможность

нарушения конфиденциальности, целостности или доступности информации, содержащейся в информационной системе и приведет ли нарушение хотя бы одного из указанных свойств безопасности информации к наступлению неприемлемых негативных последствий.

Обзор текущего состояния

Базы данных угроз и реестры уязвимостей с практической точки зрения полезны специалистам в области информационной безопасности. Систематический мониторинг БДУ ФСТЭК позволяет сотрудникам информационной безопасности своевременно узнавать о появлении новых угроз и оперативно принимать меры по реагированию на актуальные угрозы исходя из оценки критичности уязвимого программного обеспечения. Также значимыми характеристиками будут наличие рекомендаций по устранению уязвимостей и возможность определения потенциальных векторов атак на защищаемые информационные ресурсы.

Таким образом, моделирование угроз безопасности информации на основе данных банка угроз безопасности (БДУ) ФСТЭК является целостным и структурированным процессом, который учитывает особенности функционирования различных типов информационных систем.

Выводы.

Актуальность информации и выводы, приведенные в статье очевидны т.к. процесс моделирования угроз - это итеративный процесс, позволяющий определить актуальные угрозы, которые в случае реализации могут быть критичными для ценных активов предприятия и могут привести к серьёзному ущербу. Определение актуальных угроз так же является доказательным фактом для создания требуемого уровня защиты информации, установления приоритетов в планировании бюджета на обеспечение ИБ и дает для руководства компаний понимание о необходимости модернизации системы защиты. Кроме того, моделирование угроз может помочь обеспечить адекватность поддержания требуемого уровня защиты информации. Надеемся, что изложенные в статье информация найдет понимание в различных сферах образования для студентов и преподавателей, а также возможность практического применения материала статьи для специалистов по защите информации организаций.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Методика оценки угроз безопасности: методический документ / сост. ФСТЭК России. – Москва, 2021. – 83 с.
3. Positive Technologies. Вебсайт. Москва, 2002. Режим доступа: https://www.ptsecurity.
4. Информационно-аналитический журнал «RUБЕЖ» [Электронный ресурс]. – Москва. – 2013 г. – Режим доступа : htps://ru-bezh.ru.
5. Ландшафт угроз для систем промышленной автоматизации. Kapersky ICS CERT. [Электронный ресурс]: – Режим доступа: htts://icscert.kaspersky.ru/media/H1_2019_kaspersky_ICS_REPORT_RUS.
6. Закон РФ от 27.07.2006 г. №152-ФЗ «О персональных данных».
7. Приказ ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
8. Приказ ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
9. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

10. «Приоритетные направления развития науки, технологий и техники в Российской Федерации и перечень критических технологий Российской Федерации». Утверждены Указом Президента Российской Федерации от 7 июля 2011 года № 899.

11. Постановление Правительства Российской Федерации от 24 октября 2011 г. №861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг».

12. https://attack.mitre.org/matrices/enterprise/

13. https://mitre-attack.github.io/attack-navigator/

14. https://apt.securelist.com

15. https://fstec.ru/

REFERENCES

1. Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies and Information Protection".

2. Methodology for assessing security threats: methodological document / comp. FSTEC of Russia. - Moscow, 2021. - 83 p.

3. Positive Technologies. Website. Moscow, 2002. Access mode: https://www.ptsecurity .

4. Information and analytical journal "RUBEZH" [Electronic resource]. - Moscow. - 2013 - Access mode : https://ru-bezh.ru.

5. Threat landscape for industrial automation systems. Kapersky ICS CERT. [Electronic resource] – Access mode: https://icscert.kaspersky.ru/media/H1_2019_kaspersky_ICS_REPORT_RUS.

6. The Law of the Russian Federation of 27.07.2006 No. 152-FZ "On personal data".

7. The Order of the FSTEC of Russia of February 11, 2013 No. 17 "On approval of requirements for the protection of information not constituting a state secret contained in state information systems".

8. Order of the FSTEC of Russia No. 21 dated February 18, 2013 "On Approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems".

9. Decree of the Government of the Russian Federation No. 1119 dated 01.11.2012 "On Approval of requirements for the protection of personal data during their processing in information systems personal data".

10. "Priority directions of development of science, technology and engineering in the Russian Federation and the list of critical technologies of the Russian Federation". Approved by Decree of the President of the Russian Federation No. 899. 11 of July 7, 2011

11. Decree of the Government of the Russian Federation No. 861 of October 24, 2011 "On Federal State Information Systems Providing the provision of State and Municipal services in Electronic Form".

12. https://attack.mitre.org/matrices/enterprise/

13. https://mitre-attack.github.io/attack-navigator/

14. https://apt.securelist.com

15. https://fstec.ru/

Информация об авторе

Серёдкин Сергей Петрович – к. э. н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: sseryodkin2008@yandex.ru.

Author

Seryodkin Sergei Petrovich – Ph. D. in Economics, Associate Professor, the Subdepartment of Information systems and information security, Irkutsk State Transport University, Irkutsk, e-mail: sseryodkin2008@yandex.ru.

Для цитирования

Серёдкин С.П. Моделирование угроз безопасности информации на основе банка угроз ФСТЭК России // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2022. – №1(13). – С. 43-54 – DOI: 10.26731/2658-3704.2022.1(13).43-54 – Режим доступа: http://ismm-irgups.ru/toma/113-2022, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 26.04.2022)

For citations

Seryodkin S.P. Scientific approaches to the justification of investments in data security // 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], 2022. No. 1(13). P. 43-54. DOI: 10.26731/2658-3704.2022.1(13).43-54. [Accessed 26/04/22]