Научная статья
УДК 004.056; DOI: 10.61260/2218-13X-2025-1-81-93

ПРОБЛЕМНЫЕ ВОПРОСЫ НОРМАТИВНО-ПРАВОВОГО ИНСТРУМЕНТАРИЯ И АВТОРСКАЯ МЕТОДИКА АКТУАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ И КИБЕРБЕЗОПАСНОСТИ

✉Буйневич Михаил Викторович;
Чурилина Валерия Валерьевна.
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉bmv1958@yandex.ru

Аннотация. Работа посвящена решению задачи актуализации угроз информационной и кибербезопасности для информационной инфраструктуры, информационных систем и ресурсов МЧС России. Показано, что условия ее решения на сегодня отличаются от «статичных» и однозначно регламентированных, что порождает целый ряд проблемных вопросов нормативно-правового инструментария и переводит ее в ранг сложной научно-технической задачи. Установлен факт смены Регулятором основания систематизации угроз безопасности информации, что привело к сокращению мощности их множества с 222 до 11 и инновационному подходу к разработке авторской методики актуализации угроз. Изложены ее шаги: 1) составление экспертной анкеты в нотации базы данных угроз Регулятора; 2) опрос экспертов с заполнением анкеты в электронном виде; 3) сведение результатов опроса в таблицу с суммированием частоты применения каждого из 171 способа реализации угроз; 4) соотнесение «актуальных» способов с потенциально реализуемыми ими угрозами и суммирование частоты применения по всему пулу способов; 5) построение гистограммы рейтингования угроз информационной и кибербезопасности для информационной инфраструктуры, информационных систем и ресурсов МЧС России для всех 11 угроз. Сделаны выводы относительно новизны и практической значимости полученных результатов, а также направления дальнейших исследований.

Ключевые слова: информационная и кибербезопасность, угрозы безопасности информации, способы реализации угроз, база данных угроз Регулятора, методика актуализации угроз, рейтингование

Для цитирования: Буйневич М.В., Чурилина В.В. Проблемные вопросы нормативно-правового инструментария и авторская методика актуализации угроз информационной и кибербезопасности // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2025. № 1. С. 81–93. DOI: 10.61260/2218-13X-2025-1-81-93.

Scientific article

REGULATORY AND LEGAL INSTRUMENTS` PROBLEMATIC ISSUES AND AUTHOR'S TECHNIQUE FOR ACTUALIZATION OF INFORMATION AND CYBER SECURITY THREATS

✉Buinevich Mikhail V.;
Churilina Valeria V.
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉bmv1958@yandex.ru

Abstract. The work is devoted to solving the problem of information and cyber security threats actualization to EMERCOM of Russia information infrastructure, information systems and resources. It has been demonstrated that the conditions under which it is solve in the present day differ from those of a «static» and unambiguously regulated system. This has resulted in the emergence of a number of regulatory and legal instruments` problematic issues and

has consequently elevated it to the rank of a complex scientific and technical task. It has been demonstrated that the Regulator has altered the basis for the systematization of information security threats. This led to a reduction in the power of their set from 222 to 11 and inspired an innovative approach to developing an authoring technique for threat actualization. Its steps are outlined: 1) preparation of an expert questionnaire in the notation of the Regulator's threat database; 2) interviewing the experts and filling in the questionnaire in electronic form; 3) compiling the interview results into a table, the objective of which is to summarize the frequency with which each of the 171 ways of realizing threats was applied; 4) correlation of «actual» ways with potentially realizable threats and summating of how often each way is used; 5) construction of a histogram of the information and cyber security threat assessment of EMERCOM of Russia information infrastructure, information systems and resources for all 11 threats. Conclusions are drawn regarding the novelty and practical significance of the results obtained, as well as directions for further research.

Keywords: information and cyber security, threats to information security, threat realization ways, Regulator's threat database, threat actualization technique, ranking

For citation: Buinevich M.V., Churilina V.V. Regulatory and legal instruments` problematic issues and author's technique for actualization of information and cyber security threats // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2025. № 1. P. 81–93. DOI: 10.61260/2218-13X-2025-1-81-93.

Введение

Информационная инфраструктура, информационные системы и ресурсы МЧС России подвергаются значительному количеству угроз безопасности информации (УБИ), вектор которых имеет тенденцию расширяться, особенно в свете последних событий. Реализация УБИ приводит к нарушениям информационной и кибербезопасности и нанесению ущерба конфиденциальности, целостности и доступности информационных ресурсов.

Согласно целевому предназначению, требования (точнее – их выполнение, соблюдение) информационной и кибербезопасности, генерируемые Регуляторами[1], как раз и направлены на нейтрализацию (блокирование) УБИ. Их (требований) выполнение (соблюдение) в подразделениях, на которые возложена задача по обеспечению безопасности информации, предполагает реализацию соответствующих организационных и технических мер по защите информации.

Последние являются затратными по всем измерениям привлекаемых для этого ограниченных ресурсов (временны́х, финансовых, людских и проч.), отсюда – их приложение (привлечение) для борьбы с неактуальными угрозами недопустимо. Поэтому на должных лиц, ответственных за обеспечение безопасности информации, возлагается миссия по определению пула актуальных из множества УБИ, что является достаточно рутинной, правда, с элементами эвристики, но все же инженерной задачей ввиду наличия соответствующих документов методического характера от Регуляторов. Однако условия ее решения на сегодня отличаются от «статичных» и однозначно регламентированных, что порождает целый ряд проблемных вопросов нормативно-правового инструментария[2], и переводит ее в ранг сложной научно-технической задачи.

[1] Регуляторами в области информационной и кибербезопасности являются Федеральная служба по техническому и экспортному надзору (ФСТЭК) России, ФСБ России и Роскомнадзор

[2] Это понятие введено в научный оборот в статье Шеремет Н.М., Епишкин И.А. Влияние нормативно-правового инструментария на управление персоналом организации // Право и государство: теория и практика. 2017. № 10 (154). С. 145–148] и трактуется как совокупность юридических техник, используемых при выработке, систематизации и совершенствовании нормативных правовых актов

В этой связи исследование этих вопросов и производного от них методического инструментария актуализации угроз информационной и кибербезопасности для информационной инфраструктуры, информационных систем и ресурсов МЧС России является актуальным.

Проблемные вопросы актуализации угроз в контексте требований информационной и кибербезопасности

Оценка актуальности УБИ производится в соответствии с методическим документом [1][3]. Согласно п. 5.3.2 методического документа «*Исходными данными для оценки актуальности угроз безопасности информации являются:*

а) общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

б) описания векторов компьютерных атак, содержащихся в базах данных и иных информационных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);

в) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей методикой (методическим документом);

г) объекты воздействия угроз безопасности информации и виды воздействий на них, определенные в соответствии с настоящей методикой (методическим документом);

д) виды и категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы, и их возможности, определенные в соответствии с настоящей методикой (методическим документом);

е) актуальные способы реализации (возникновения) угроз безопасности информации».

Рассмотрим общий перечень УБИ на предмет решения поставленной задачи – актуализации угроз информационной и кибербезопасности для информационной инфраструктуры, информационных систем и ресурсов МЧС России.

Актуализация авторами понимается в широком смысле слова, как процесс приведения пула УБИ в соответствие с современными условиями выполнения требований информационной и кибербезопасности в подразделениях МЧС России, на которые возложена эта задача.

Согласно пп. а методического документа, «*общий перечень угроз безопасности информации содержится в* одноименном *банке данных ФСТЭК России (bdu.fstec.ru)*».

Однако сайт ФСТЭК бóльшую часть 2024 г. и на момент написания статьи находится в режиме модернизации, которая, в частности, для ключевой сущности сферы **информационной и кибербезопасности** – «угрозы» – заключается в том, что наряду с «традиционным» перечнем (Перечень_1) УБИ (УБИ_*n*, $n \in N$) общим количеством $N = 222$, в рубрике «Угрозы» появился новый раздел угроз с одноименным названием, общим количеством $N = 11$ (Перечень_2) .

В настоящее время проводится опытная эксплуатация модернизированного раздела угроз со сбором замечаний и предложения по его работе. Этот факт имеет большое значение для всей отрасли информационной безопасности и защиты информации по целому ряду обстоятельств, но принципиальным для выполнения задачи актуализации угроз информационной и кибербезопасности является смена основания систематизации УБИ.

[3] Далее по тексту цитаты из методического документа приводятся «*курсивом и в кавычках*».

Так, если в первом случае (Перечень_1) основанием является способ нанесения ущерба конфиденциальности, целостности и/или доступности информации в связи с наступлением негативных последствий (например, УБИ.005 – Угроза внедрения вредоносного кода в BIOS – которая заключается в возможности заставить BIOS/UEFI выполнять вредоносный код при каждом запуске компьютера, внедрив его в BIOS/UEFI путём замены микросхемы BIOS/UEFI или обновления программного обеспечения BIOS/UEFI на версию, уже содержащую вредоносный код), то во втором (Перечень_2) – «целевой способ» ее реализации (например, УБИ.4 – Угроза несанкционированной подмены – которая заключается во внедрении ложного или подмене существующего компонента информационной системы и (или) обрабатываемой с его использованием информации.

Понятие «целевой способ» взято авторами в кавычки и требует трактовки. Покажем смысл, который вкладывается в это понятие на примере вышеприведенной УБИ.4. Несанкционированная подмена не является самоцелью нарушителя; его конечной целью является нарушение одного из трех свойств защищаемой информации – конфиденциальности и/или целостности и/или доступности. Внедрение ложного или подмена существующего компонента информационной системы и (или) обрабатываемой с его использованием информации раскрывает (в общих чертах) каким образом (способом) нарушитель собирается реализовать эту угрозу. Таким образом, основанием для Перечня_2 является промежуточная цель и укрупненный способ ее реализации.

Другие (альтернативные) основания систематизации также могут быть как информационными хранилищами Best Practices, так и источником (пусть пока теоретических) знаний об условно новых (объективно существующих, но не декларируемых ввиду отсутствия разработанного понятийного аппарата) классах угроз и способах борьбы с ними. В этом плане не только теоретический, но и сугубо практический интерес представляет класс угроз межмодульного информационного взаимодействия в интегрированной системе защиты информации (ИСЗИ), впервые описанный в работах М.В. Буйневича, К.Е. Израилова и В.В. Покусова [2, 3]. Результатом авторских исследований стали шесть основных угроз класса «УИВ» (угроза информационного взаимодействия), приводящих к нарушениям информационной безопасности и снижению работоспособности ИСЗИ после интеграции в нее различных подсистем защиты информации. Описание угроз в аналитическом виде (в нотации логики предикатов), а затем отрицание условий их существования, позволило перевести требования защиты информации в ИСЗИ в научно-обоснованные.

Еще одним метаклассом УБИ выступают, так называемые, «комбинированные» атаки, которые, с очевидностью, предполагают и комбинирование способов противодействия. Специалисты по информационной безопасности и защите информации трактуют это понятие и как расширенные угрозы (и реализующие их атаки); «продвинутые», «развитые», «сложные», «целевые», «целенаправленные» и «таргетированные». Однако истинный смысл состоит в том, что для нарушения относительного паритета «атака vs защита» злоумышленники усиливают натиск на системы обеспечения безопасности информации, комбинируя разнородные деструктивные воздействия, затрудняя тем самым способность к противодействию. Несмотря на значительное количество публикаций, посвященных подобному информационному противоборству, каких-либо научных исследований, посвященных анализу этого относительно нового явления в части выявлению границ комбинирования, а также способности к противодействию возможным комбинациям в открытом доступе не наблюдается. В работах М.В. Буйневича и Г.Ю. Моисеенко [4–6] исследуется феномен комбинирования разнородных деструктивных воздействий на информационную систему и противодействия таким атакам. В интересах классификации и выделения таких атак применяется аппарат категориального деления. Впервые рассматривается комбинация двух, на первый взгляд, несвязанных, деструктивных воздействий – инсайдерской деятельности и DDoS-атаки. Также в научный оборот вводится понятие «неумышленный инсайдинг» и рассматривается принципиально новый класс уязвимостей организационной/информационной системы – «неустойчивость» регламентов деятельности сотрудников (инструкций).

Перечень_1 в настоящее время применяется в МЧС России (и не только) для формирования должностными лицами, ответственными за информационную безопасность и защиту информации, частных моделей (актуальных) угроз информационным системам и ресурсам, а также, в том числе, для аттестации сегментов цифровой информационной инфраструктуры МЧС России по требованиям безопасности информации.

Оба эти прикладных приложения Перечня_1 представляют, хотя с элементами эвристики, но все же инженерную и достаточно частную задачу, которая достаточно успешно решается «на местах» с использованием вышеуказанного методического документа. Однако здесь существуют как минимум два проблемных вопроса.

Во-первых, если чисто гипотетически предположить, что актуализация УБИ в масштабах ведомства (то есть, формирование ведомственной модели угроз) есть некая агрегация частных моделей (актуальных) угроз, разрабатываемых и разработанных «на местах» – то есть синтез «модели моделей», то:

– для решения подобного масштаба многофакторных, многокритериальных и причем слабоформализованных задач отсутствует готовый инструментарий (а его разработка представляется сверхсложной);

– у такой модели будет нарушено свойство адекватности, поскольку она будет соответствовать настолько абстрактному объекту (по типу «сферического коня в вакууме»), что ее прагматичность устремится к нулю.

Во-вторых, в разработанных лицензиатами ФСТЭК России Требованиях к сегменту цифровой информационной инфраструктуры МЧС России – документу, определяющему условия и порядок распространения действующих Аттестатов соответствия по требованиям безопасности информации, в качестве обязательного структурного элемента присутствует перечень актуальных (для конкретной информационной системы – ИС) угроз в нотации и из состава Перечня_1. Например, для ИС «Система электронного документооборота МЧС России», дословно из работы [7]): «*1.7. В «Модели угроз и потенциального нарушителя безопасности данных при их обработке в Системе электронного документооборота МЧС России ИС» был определен .... перечень* ***актуальных УБИ***» (в настоящей статье не приводится по причине конфиденциальности содержания, а угрозы условно промаркированы знаком «*»):

Таблица ***

Перечень актуальных угроз безопасности информации ИС «СЭД МЧС России»

№ п/п	Идентификатор угрозы	Наименование угрозы
1	УБИ.***	Угроза ***
2	УБИ.***	Угроза ***
3	УБИ.***	Угроза ***
…	…	…
44	УБИ.***	Угроза ***
45	УБИ.***	Угроза ***

Тогда результаты любой сторонней актуализации УБИ по Перечню_1, не совпадающие «суммарно» с аттестатами соответствия всех эксплуатируемых в МЧС России сегментов, ставят под сомнение компетентность как экспертного сообщества, так и лицензиатов ФСТЭК России.

В этих условиях в качестве объекта актуализации УБИ может быть выбран Перечень_2, являющийся результатом более «продвинутого» в методологическом плане подхода к систематизации, который после модернизации официального сайта Регулятора либо заменит собой Перечень_1, либо последний будет служить только справочным материалом как информационное хранилище Best Practices.

Так как в результате модернизации базы данных угроз (БДУ) пул УБИ (в результате смены основания систематизации) сократился с 222 до 11, это повлекло за собой кардинальное изменение «статуса» УБИ.

В отличие от 222, где далеко не все УБИ из Перечня_1 идентифицируются на объектах информатизации (ИС, автоматизированные системы (АС), сегментах и т.п.) МЧС России, и можно говорить о подмножестве актуальных угроз, то в противовес – все 11 УБИ из Перечня_2 будут идентифицироваться на любом объекте информатизации.

Действительно, формулировки УБИ из Перечня_2 (табл. 1): угроза утечки информации, несанкционированного доступа, несанкционированной модификации (искажения), несанкционированной подмены, удаления информационных ресурсов, отказа в обслуживании и т.п. – являются достаточно укрупненными, чтобы быть идентифицированными практически повсеместно (имеется в виду – информационные системы).

Таблица 1

Перечень_2 УБИ

Идентификатор угрозы	Наименование угрозы	Формулировка угрозы
УБИ.1	Угроза утечки информации	Угроза заключается в возможности противоправного получения либо передачи информации (конфиденциальной, конфигурационной, аутентификационной и др.)
УБИ.2	Угроза несанкционированного доступа	Угроза заключается в получении доступа к информационным ресурсам, нарушающего установленные в информационной системе правила разграничения доступа
УБИ.3	Угроза несанкционированной модификации (искажения)	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
УБИ.4	Угроза несанкционированной подмены	Угроза заключается во внедрении ложного или подмене существующего компонента информационной системы и (или) обрабатываемой с его использованием информации
УБИ.5	Угроза удаления информационных ресурсов	Угроза заключается в несанкционированном удалении обрабатываемой в информационной системе информации (конфиденциальной, конфигурационной, аутентификационной и др.)
УБИ.6	Угроза отказа в обслуживании	Угроза заключается в недоступности информационной системы или ее компонентов и (или) приостановлении оказания услуг или предоставления сервисов для авторизованных пользователей
УБИ.7	Угроза ненадлежащего (нецелевого) использования	Угроза заключается в использовании вычислительных ресурсов средств вычислительной техники для осуществления сторонних, не предусмотренных технологией обработки информации, процессов
УБИ.8	Угроза нарушения функционирования (работоспособности)	Угроза заключается в частичной или полной утрате работоспособности или функциональности компонента или информационной системы в целом
УБИ.9	Угроза получения информационных ресурсов	Угроза заключается в нарушении функционирования информационной системы и (или) внедрении в ее состав вредоносных программных или

Идентификатор угрозы	Наименование угрозы	Формулировка угрозы
	из недоверенного или скомпрометированного источника	программно-аппаратных средств в результате получения компонентов информационной системы из недоверенных (происхождение или принадлежность которого неизвестны) или легитимных скомпрометированных источников
УБИ.10	Угроза распространения противоправной информации	Угроза заключается в распространении противоправной информации с применением информационной системы или ее компонентов, а также в возможности осуществления с их использованием вредоносного воздействия на другие информационные системы
УБИ.11	Угроза несанкционированного массового сбора информации	Угроза заключается в несанкционированном сборе информации, обрабатываемой информационной системой или ее компонентами, с использованием автоматизированных средств сбора данных (\\«парсеров\\», скриптов автоматизации и др.)

Таким образом, все УБИ из Перечня_2 должны быть признаны актуальными – то есть подлежащими нейтрализации (блокированию).

Однако ограниченность ресурса, выделяемого ведомством на реализацию организационных и технических мер по защите информации, не позволит его использовать «на местах» мгновенно и для борьбы со всеми актуальными угрозами, то есть индуцируется естественный вопрос о приоритетности реализации мер и соответственно нейтрализуемых (блокируемых) (минимизируемых) актуальных угроз.

Можно предположить, что в первую очередь нейтрализации (блокированию) подлежат УБИ, которые потенциально наносят бóльший ущерб безопасности информации и имеют бóльшую частоту (вероятность) реализации.

Примечание: хотя в связи с утверждением методического документа, Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [8], утвержденная ФСТЭК России 14 февраля 2008 г., не применяется для оценки УБИ, однако в научном-методологическом плане вполне допустимо ее использование в качестве терминологической Best Practice.

Согласно работе [8], под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной УБИ для данной ИС в складывающихся условиях обстановки. Тогда предметом актуализации УБИ для информационной инфраструктуры, информационных систем и ресурсов МЧС России будет являться их рейтингование по частоте (вероятности) реализации.

Согласно п. 5.3.4 методического документа «*Актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации. Сценарии реализации угроз безопасности информации должны быть определены для соответствующих способов реализации угроз безопасности информации*».

Согласно п. 5.3.5 методического документа «*Сценарий определяется для каждого актуального нарушителя и их уровней возможностей. При наличии хотя бы одного сценария угрозы безопасности информации такая угроза признается актуальной ... и включается в модель угроз безопасности ... для обоснования выбора организационных и технических мер по защите информации (обеспечению безопасности), а также выбора средств защиты информации*».

То есть актуальность УБИ есть функция (вероятностная) наличия сценария, который определяется через соответствующие способы (применительно к объектам и видам воздействия).

В Перечне_2, организованном по типу реляционной БД, установлено однозначное соответствие между угрозой и способом(ами) ее реализации, например:

Угроза	Способы (СП) реализации
УБИ.4 Угроза несанкционированной подмены	СП.1.1 Эксплуатация известных уязвимостей; СП.1.2 Эксплуатация уязвимостей «нулевого дня»; СП.2.1 Использование недостатков, связанных с неполнотой проверки вводимых (входных) данных; СП.2.2 Использование недостатков, связанных с управлением учетными данными; .... СП.25.3 Атаки на смарт-контракты; СП.25.4 Атаки на услуги системы с распределенным реестром

и наоборот:

Способ реализации угрозы	Возможные реализуемые угрозы
СП.22.28 Переполнение буфера	УБИ.2 Угроза несанкционированного доступа; УБИ.3 Угроза несанкционированной модификации (искажения); УБИ.4 Угроза несанкционированной подмены; УБИ.5 Угроза удаления информационных ресурсов; УБИ.7 Угроза ненадлежащего (нецелевого) использования; УБИ.8 Угроза нарушения функционирования (работоспособности); УБИ.10 Угроза распространения противоправной информации; УБИ.11 Угроза несанкционированного массового сбора информации

Тогда, определив возможные способы (а они не все являются равновозможными) реализации (возникновения) угроз, можно будет рассчитать частоту реализации конкретной УБИ из 11, то есть отранжировать Перечень_2.

Для реализации этой идеи потребуется соответствующий инструментарий в виде Методики рейтингования угроз информационной и кибербезопасности для информационной инфраструктуры, информационных систем и ресурсов МЧС России (Методика).

Методика рейтингования угроз информационной и кибербезопасности для информационной инфраструктуры, информационных систем и ресурсов МЧС России

Согласно п. 2.8 методического документа «*Оценка угроз безопасности информации проводится с использованием экспертного метода. В интересах снижения субъективных факторов при оценке угроз безопасности информации рекомендуется создавать экспертную группу*». Поэтому для решения задачи рейтингования выбран экспертный метод.

С учетом выбранного и обоснованного метода решения задачи рейтингования суть Методики заключается в составлении анкеты, содержащей список возможных способов реализации УБИ, исходящих как от сети Интернет (для систем, имеющих выход в сети общего доступа), так и от сети Интранет (подключенных только к локальной сети организации), и ее заполнении экспертами путем выбора того или иного способа

применительно к информационной инфраструктуре, информационным системам и ресурсам МЧС России для конкретной организации, с последующей обработкой и отображением результатов, – что и определяет содержание Методики.

Согласно рекомендациям, изложенным в Приложении 2 методического документа, в состав экспертной группы для оценки УБИ были включены представители от подразделений:

– по защите информации (обеспечению информационной безопасности);

– ответственных за эксплуатацию сетей связи, ИС и АС;

– обладателя информации или оператора, ответственного за выполнение информационных процессов («ключевых» пользователей).

Все специалисты из состава экспертной группы имеют опыт работы не менее одного года по соответствующему направлению деятельности.

Для снижения предвзятости и устранения давления на принимаемые решения у всех экспертов отсутствовал финансовый или иной коммерческий интерес; также в составе экспертной группы отсутствовали участники, находящиеся в прямом подчинении.

Для организации работы экспертной группы был определен ученый-специалист по защите информации (обеспечению информационной безопасности), имеющий стаж работы по профилю свыше 20 лет и практический опыт оценки информационных рисков.

Примечание: так как оригинальные результаты рейтингования угроз информационной и кибербезопасности для информационной инфраструктуры, информационных систем и ресурсов МЧС России являются конфиденциальной информацией, то далее по тексту для демонстрации последовательности и доказательства работоспособности Методики использованы условные данные, полученные с использованием программного датчика случайных чисел.

Методика является пошаговой.

Шаг_1. На этом шаге составляется экспертная анкета, специально разработанная авторами для решения задачи рейтингования угроз информационной и кибербезопасности для информационной инфраструктуры, информационных систем и ресурсов МЧС России. Форма экспертной анкеты фрагментарно приведена на рис. 1.

ВОЗМОЖНЫЕ СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗ

СП.1 ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ
☒СП.1.1 Эксплуатация известных уязвимостей
☐СП.1.2 Эксплуатация уязвимостей «нулевого дня»
… … …
СП.6 ИСПОЛЬЗОВАНИЕ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ
☐СП.6.1 Использование недекларированных возможностей аппаратных средств
☒СП.6.2 Использование недекларированных возможностей операционных систем
☒СП.6.3 Использование недекларированных возможностей прикладного программного обеспечения
… … …
СП.25 АТАКИ НА СИСТЕМЫ С РАСПРЕДЕЛЕННЫМ РЕЕСТРОМ
☐СП.25.1 Атаки на механизмы идентификации участников системы распределенного реестра
☐СП.25.2 Атаки на протоколы достижения консенсуса
☐СП.25.3 Атаки на смарт-контракты
☐СП.25.4 Атаки на услуги системы с распределенным реестром

Рис. 1

Как видно, форма разработана в нотации БДУ с однозначно трактуемыми вопросами, предполагающими однозначные ответы; обработка результатов ее заполнения позволяет сделать научно-обоснованные выводы относительно актуальности УБИ.

Шаг_2. На этом шаге проводится опрос экспертов с заполнением анкеты в электронном виде.

Шаг_3. На этом шаге результаты анкетирования экспертов сводятся в табл. 2, где Э.К – эксперт с условным номером К, СП.N.M – условный номер способа реализации угроз согласно раздела «Новый раздел угроз» подраздела «Справочники» пункта «Способы реализации» (https://bdu.fstec.ru/threat), с простым суммированием частоты применения способа по всем экспертам (столбец «Σ», выделен желтым фоном).

Таблица 2

Результаты анкетирования экспертов
по вопросу возможных способов реализации УБИ

№ п/п	Способы реализации угроз	Э.1	Э.2	Э.3	Э.4	Э.5	Э.6	Э.7	Э.8	Э.9	Э.10	∑
1	СП.1.1	–	1	–	–	1	–	1	1	1	–	5
2	СП.1.2	1	–	1	–	–	1	–	1	–	1	5
3	СП.2.1	1	1	1	1	1	1	1	–	1	1	9
…	…	…	…	…	…	…	…	…	…	…	…	…
52	СП.9.3	–	–	1	–	1	–	1	–	–	–	3
53	СП.9.4	1	–	1	1	–	1	–	–	1	1	6
54	СП.9.5	–	1	–	–	1	1	1	–	–	1	5
…	…	…	…	…	…	…	…	…	…	…	…	…
169	СП.25.2	–	–	–	–	1	–	1	1	1	–	4
170	СП.25.3	1	–	1	–	1	1	1	1	–	–	6
171	СП.25.4	1	–	–	1	1	1	1	–	–	–	5

Шаг_4. На этом шаге «актуальные» способы соотносятся с УБИ, потенциально реализуемые ими, для чего значения частоты применения конкретного способа по всем экспертам из столбца «Σ» табл. 2 тиражируются для всех УБИ из Перечня_2, потенциально реализуемых данным способом. Сведения о соотношении «Способ реализации» vs «Возможные реализуемые угрозы» берутся из БДУ ФСТЭК (bdu.fstec.ru); угрозы, которые потенциально не реализуются конкретным способом, отмечены в таблице темным фоном. В подстрочнике УБИ суммируется значение частоты применения по всему пулу способов (красным жирным шрифтом). Результат обработки экспертных анкет сводится в табл. 3.

Шаг_5. На этом шаге строится гистограмма рейтингования угроз информационной и кибербезопасности для информационной инфраструктуры, информационных систем и ресурсов МЧС России для всех УБИ из Перечня_2 (рис. 2). В качестве аргумента используется суммарное значение частоты возможности применения по всему пулу способов из табл. 3.

Полученные результаты позволяют сделать вывод о работоспособности Методики и сфокусировать внимание (а в последствии – и сконцентрировать ограниченный ресурс) на нейтрализацию (блокирование) УБИ, имеющих бóльшую частоту (вероятность) реализации.

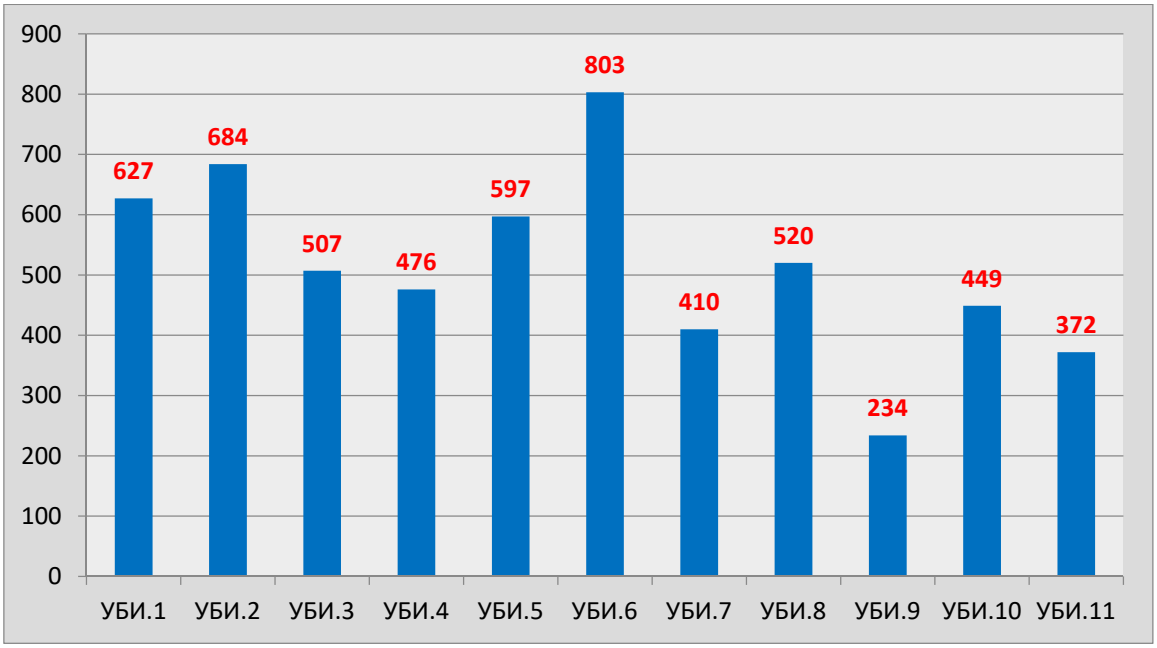

Рис. 2. **Гистограмма рейтингования УБИ**

Таблица 3

Результаты обработки экспертных анкет

№ п/п	Способ	Σ	УБИ.1	УБИ.2	УБИ.3	УБИ.4	УБИ.5	УБИ.6	УБИ.7	УБИ.8	УБИ.9	УБИ.10	УБИ.11
			627	**684**	**507**	**476**	**597**	**803**	**410**	**520**	**234**	**449**	**372**
1	СП.1.1	5	5	5	5	5	5	5	5	5		5	5
2	СП.1.2	5	5	5	5	5	5	5	5	5		5	5
3	СП.2.1	9	9	9	9	9	9	9	9	9	9	9	9
…	…	…	…	…	…	…	…	…	…	…	…	…	…
52	СП.9.3	3						3					3
53	СП.9.4	6						6					6
54	СП.9.5	5						5					5
…	…	…	…	…	…	…	…	…	…	…	…	…	…
169	СП.25.2	4	4	4	4	4	4	4	4	4	4	4	
170	СП.25.3	6	6	6	6	6	6	6	6	6	6	6	
171	СП.25.4	5	5	5	5	5	5	5	5	5	5	5	

Заключение

Выполненная авторами работа относится к отчетным материалам НИР «Разработка принципов, методологии и элементов технологии решения прикладных задач гармонизации нормативной правовой базы в части требований информационной и кибербезопасности в интересах МЧС России» (шифр «Гармония», рег. № 123030100009-7), а именно к подразделу 1.3 «Актуализация угроз информационной и кибербезопасности для информационной инфраструктуры, информационных систем и ресурсов МЧС России».

Первым научным результатом, изложенным в статье, являются вскрытые авторами проблемные вопросы предметной области, анализ которых позволил выдвинуть гипотезу: так как актуальность УБИ есть однозначная функция наличия сценария реализации способа ее возникновения, тогда определив все неравновозможные способы, можно рассчитать частоту реализации конкретной угрозы, то есть отранжировать УБИ по актуальности.

В подтверждение гипотезы получен второй научный результат – Методика рейтингования угроз информационной и кибербезопасности для информационной инфраструктуры, информационных систем и ресурсов МЧС России.

Новизна полученных результатов состоит в инновационном подходе к решению задачи актуализации УБИ, а практическая значимость – в инструментальном характере Методики. Предполагается, что доведение ее до программной реализации повысит степень автоматизации деятельности должностных лиц, ответственных за обеспечение информационной безопасности и защиту информации.

Дальнейшие исследования в этом направлении видятся на путях интеграции и активного использования Best Practices, обработанных с помощью методов искусственного интеллекта.

Список источников

1. Методика оценки угроз безопасности информации: метод. документ (утв. ФСТЭК России 5 февр. 2021 г.). Доступ из справ.-правового портала «Гарант».

2. Буйневич М.В., Израилов К.Е., Покусов В.В. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации // Информатизация и связь. 2021. № 4. С. 66–73. DOI: 10.34219/2078-8320-2021-12-4-66-73.

3. Покусов В.В. Аналитическая модель угроз межмодульного взаимодействия в системе защиты информации // Информатизация и связь. 2023. № 3. С. 76–84. DOI: 10.34219/2078-8320-2023-14-3-76-84.

4. Буйневич М.В., Моисеенко Г.Ю. Комбинирование разнородных деструктивных воздействий на информационную систему и противодействие атакам (на примере инсайдерской деятельности и DDoS-атаки) // Информационные технологии и телекоммуникации. 2023. Т. 11. № 3. С. 27–36. DOI: 10.31854/2307-1303-2023-11-3-27-36.

5. Буйневич М.В., Власов Д.С., Моисеенко Г.Ю. Комбинирование способов выявления инсайдеров больших информационных систем // Вопросы кибербезопасности. 2024. № 3 (61). С. 2–13. DOI: 10.21681/2311-3456-2024-3-2-13.

6. Буйневич М.В., Моисеенко Г.Ю. Повышение «устойчивости» регламентов деятельности как способ противодействия неумышленному инсайдингу // Вопросы кибербезопасности. 2024. № 6 (64). С. 108–116. DOI: 10.21681/2311-3456-2024-6-108-116.

7. Требованиях к сегменту информационной системы «Система электронного документооборота МЧС России» (выдан ФГБУ «Информационно-аналитический центр МЧС России» 16.06.2020 г.; лицензиат – ООО Центр защиты информации «Эгида» (лицензия ФСТЭК России № 2712 от 30 сент. 2015 г.). Доступ из справ.-правового портала «Гарант».

8. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК России 14 февр. 2008 г.). Доступ из справ.-правового портала «Гарант».

References

1. Metodika ocenki ugroz bezopasnosti informacii: metod. dokument (utv. FSTEK Rossii 5 fevr. 2021 g.). Dostup iz sprav.-pravovogo portala «Garant».

2. Bujnevich M.V., Izrailov K.E., Pokusov V.V. Model' ugroz informacionno-tekhnicheskogo vzaimodejstviya v integrirovannoj sisteme zashchity informacii // Informatizaciya i svyaz'. 2021. № 4. S. 66–73. DOI: 10.34219/2078-8320-2021-12-4-66-73.

3. Pokusov V.V. Analiticheskaya model' ugroz mezhmodul'nogo vzaimodejstviya v sisteme zashchity informacii // Informatizaciya i svyaz'. 2023. № 3. S. 76–84. DOI: 10.34219/2078-8320-2023-14-3-76-84.

4. Bujnevich M.V., Moiseenko G.Yu. Kombinirovanie raznorodnyh destruktivnyh vozdejstvij na informacionnuyu sistemu i protivodejstvie atakam (na primere insajderskoj deyatel'nosti i DDoS-ataki) // Informacionnye tekhnologii i telekommunikacii. 2023. T. 11. № 3. S. 27–36. DOI: 10.31854/2307-1303-2023-11-3-27-36.

5. Bujnevich M.V., Vlasov D.S., Moiseenko G.Yu. Kombinirovanie sposobov vyyavleniya insajderov bol'shih informacionnyh sistem // Voprosy kiberbezopasnosti. 2024. № 3 (61). S. 2–13. DOI: 10.21681/2311-3456-2024-3-2-13.

6. Bujnevich M.V., Moiseenko G.Yu. Povyshenie «ustojchivosti» reglamentov deyatel'nosti kak sposob protivodejstviya neumyshlennomu insajdingu // Voprosy kiberbezopasnosti. 2024. № 6 (64). S. 108–116. DOI: 10.21681/2311-3456-2024-6-108-116.

7. Trebovaniyah k segmentu informacionnoj sistemy «Sistema elektronnogo dokumentooborota MCHS Rossii» (vydan FGBU «Informacionno-analiticheskij centr MCHS Rossii» 16.06.2020 g.; licenziat – OOO Centr zashchity informacii «Egida» (licenziya FSTEK Rossii № 2712 ot 30 sent. 2015 g.). Dostup iz sprav.-pravovogo portala «Garant».

8. Metodika opredeleniya aktual'nyh ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh» (utv. FSTEK Rossii 14 fevr. 2008 g.). Dostup iz sprav.-pravovogo portala «Garant».

Информация о статье:
Статья поступила в редакцию: 27.12.2024; одобрена после рецензирования: 26.02.2025;
принята к публикации: 28.02.2025

The information about article:
The article was submitted to the editorial office: 27.12.2024; approved after review: 26.02.2025;
accepted for publication: 28.02.2025

Информация об авторах:
Буйневич Михаил Викторович, профессор кафедры прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), доктор технических наук, профессор, e-mail: bmv1958@yandex.ru, https://orcid.org/0000-0001-8146-0022, SPIN-код: 9339-3750,
Чурилина Валерия Валерьевна, адъюнкт факультета подготовки кадров высшей квалификации Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149). e-mail: v_v_ch97@mail.ru, SPIN-код: 1012-6413

Information about authors:
Buinevich Mikhail V., professor department of applied mathematics and information technologies of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), doctor of technical sciences, professor, e-mail: bmv1958@yandex.ru, https://orcid.org/0000-0001-8146-0022, SPIN: 9339-3750
Churilina Valeria V., adjunct of highly qualified personnel training faculty of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), e-mail: v_v_ch97@mail.ru, SPIN: 1012-6413