УДК 004.056.5 Вестник УрФО № 3(49) / 2023, с. 68–80

Повышев А.А., Соколов А.Н., Мищенко Е.Ю. DOI: 10.14529/secur230307

УНИВЕРСАЛЬНАЯ КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ЕЁ ПРИМЕНЕНИЕ ДЛЯ РАЗРАБОТКИ МОДЕЛИ УГРОЗ И ОЦЕНКИ РИСКОВ

Проведён анализ отечественных и зарубежных научных исследований и нормативно-правовых актов Российской Федерации по вопросу классификации угроз безопасности информации. В результате анализа сделан вывод об отсутствии универсальной классификации. Разработана универсальная классификация с учётом проведённого анализа и правил общей теории классификации. Предложена методика расчёта количественной оценки риска реализации угроз безопасности информации, представлены 4 примера расчёта уровня рисков для информационной системы с применением предложенной универсальной классификации.

Ключевые слова: *универсальная классификация, угрозы безопасности информации, риски информационной безопасности, расчёт рисков, банк данных угроз.*

Povyshev A.A., Sokolov A.N., Mischenko E.Yu.

UNIVERSAL CLASSIFICATION OF THREATS TO INFORMATION SECURITY AND ITS APPLICATION TO THE DEVELOPMENT OF A THREAT MODEL AND RISK ASSESSMENT

An analysis of domestic and foreign scientific research and normative legal acts of Russia on the classification of information security threats. The analysis concludes that there is no universal classification at present. We developed a universal classification taking into account the analysis and the rules of the general theory of classification. A methodology for calculating a

quantitative assessment of the risk of the implementation of information security threats is proposed, 4 examples of calculating the level of risks for the information system using the proposed universal classification are presented.

Keywords: *universal classification, information security threats, information security risks, risk calculation, threat data bank.*

Введение

Угроза информационной безопасности – это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [1]. Такая угроза определяется негативным действием, выполняемым источником по отношению к некоторому активу [2]. Банк данных угроз безопасности информации ФСТЭК России (далее – БДУ) содержит 222 позиции [3] и представляет собой обобщенный перечень угрозы безопасности информации. БДУ применяется для исследования угроз и определения их актуальности в государственных, муниципальных информационных системах (далее – ГИС, МИС) и на объектах критической информационной инфраструктуры (далее – объекты КИИ). Перечень угроз конкретной информационной системы устанавливается частной моделью угроз. Перечень угроз обновляется на регулярной основе, вместе с тем не является исчерпывающим, что отмечается ФСТЭК России [3].

Существующая нормативная база ориентирована на работу с антропогенными угрозами в ГИС, МИС и объектах КИИ. БДУ не содержит ряда потенциальных угроз, связанных с природными и политическими рисками. Действующая методика оценки [4] рассматривает только антропогенные угрозы, то есть обусловленные действиями нарушителей.

Вследствие природных или техногенных катастроф может быть утрачена информация, хранимая в информационных системах, размещённых на пострадавшей территории. С 2000 года произошло 348 наиболее разрушительных землетрясений магнитудой более 7 баллов в различных регионах мира [5]. Проблему также представляют наводнения. Катастрофические явления, вызванные наводнениями, составляют 19% от общего числа природных катастроф, они занимают первое место в ряду стихийных бедствий по повторяемости, охвату территории и материальному ущербу [6]. По данным Научного центра по эпидемиологическим катастрофам (CRED) Брюсселя количество техногенных катастроф с 1980 года по 2020 выросло в три раза [7]. Эти угрозы выделены в отдельные классы угроз, так как их возникновение не всегда является следствием злого умысла или прямого воздействия человека.

Для исследования всего многообразия угроз разработана универсальная классификационная структура, которая послужит источником знаний, позволяющим организовать систематизированное представление угроз безопасности информации и обозначить структурированные связи между ними [8].

Анализ публикаций

Российское законодательство не содержит универсальной классификации угроз безопасности информации. Вместе с тем некоторые официальные источники классифицируют угрозы по индивидуальным признакам. Доктрина информационной безопасности Российской Федерации выделяет внешние и внутренние угрозы, связанные с использованием информационных технологий в военно-политических целях [9]. ФСТЭК России делит угрозы по источнику, объекту воздействия и последствиям [3]. Базовая модель угроз безопасности персональных данных [10], применяемая наряду с Методикой оценки угроз безопасности информации [4], классифицирует угрозы по виду защищаемой информации, видам источников угроз, типу защищаемой системы, способу реализации угрозы, виду нарушаемого свойства защищаемой информации, используемой злоумышленником уязвимости и объекту воздействия.

Вопрос разработки универсальной классификации угроз безопасности информации в научных публикациях отдельно не поднимается. Как правило, авторы предлагают несколько классов угроз в рамках тематики своей публикации.

В [11] угрозы делятся на естественные и искусственные. Искусственные, в свою очередь, делятся на случайные и умышленные. К естественным отнесены угрозы воздействий стихийных природных явлений, к искусственным – угрозы, вызываемые человеком. К слу-

чайным относятся ошибки проектирования, разработки программного обеспечения, сбои технических средств, линий связи и энергоснабжения, а также ошибки, связанные с человеческим фактором.

В [12] угрозы делятся на непреднамеренные и преднамеренные. Непреднамеренные угрозы являются результатом стихийных бедствий, сбоев технических средств, ошибок при разработке, ошибок пользователей и обслуживающего персонала, ошибок в комплексах алгоритмов и программ. Преднамеренные угрозы – результат шпионажа и диверсии, несанкционированного доступа, съёма электромагнитных излучений и наводок, несанкционированной модификации, работы вредоносных программ.

В статье «Классификация угроз информационной безопасности» авторы предлагают следующие угрозы: информационные, физические, радиоэлектронные, программные и организационно-правовые [13]. Выделяются также угрозы нарушения свойств информационной безопасности –конфиденциальности, целостности и доступности.

Среди ранних отечественных публикаций на тему классифицирования угроз можно выделить работу [14], где угрозы делятся по виду ущерба: моральный, материальный, физический, финансовый; по действию злоумышленника с информацией: хищение, уничтожение, модификация (искажение), нарушение доступности (блокирование), отрицание подлинности, навязывание ложной информации; по источнику угрозы: антропогенный, техногенный, стихийные (пожары, землетрясения, наводнения, ураганы, форс-мажорные обстоятельства).

В статье «Classification of personal data security threats in information systems» угрозы персональных данных делят на угрозы, которые нельзя соотнести с атаками, и угрозы, которые могут быть соотнесены с атаками [15]. К первым авторы относят стихийные бедствия и природные явления, угрозы социально-политического характера, ошибочные действия и (или) нарушение требований со стороны персонала и пользователей, аварии, различные неисправности, помехи, вызванные различными устройствами; ко вторым – угрозы, вызванные злым умыслом человека.

В статье «Угрозы в области хранения данных» [16] авторы классифицируют угрозы безопасности информации для систем хранения данных, выделяя крупные инфраструктурные угрозы: пространственные – возникающие вследствие нехватки дискового пространства; коммуникативные – связанные с прекращением доступа к информации; деструктивные – вызванные утерей или уничтожением информации.

Зарубежные публикации обращают внимание на угрозы несанкционированного интеллектуального анализа данных, кражи носителей информации и несанкционированного доступа [17]. В статье [18] авторы исследуют угрозы интеллектуальных сетей связи, классифицируя угрозы по источнику: технические и нетехнические. К первым отнесены угрозы безопасности инфраструктуры питания, угрозы при проведении технических процедур по обслуживанию системы, угрозы при управлении системой, ко вторым отнесены угрозы, связанные с безопасностью экосистемы и правовым регулированием. Модель ISO предлагает пять угроз безопасности: угрозы уничтожения информации, искажения или модификации информации, кражи информации, удаления или утери информации, раскрытия информации; и прерывания предоставления услуг [19].

Встречаются иные формы классификации:

– модель Кьерланда делит угрозы по методу вторжения, мере воздействия, источнику вторжения и цели вторжения [20];

– таксономия Лапри классифицирует угрозы на угрозы неисправности, угрозы ошибки и угрозы сбоя [21];

– трехмерная ортогональная размерная модель угроз (Three Orthogonal Dimensional Model) предлагает разделить угрозы на три подпространства: мотивация угрозы, её локализация и агент [22];

– модель классификации «Fariborz» делит угрозы на два класса: по агенту угрозы и техники проникновения [23];

– модель Кишора выделяет четыре класса угроз: атаки-сбои (программные баги), ошибки (перегрузка, неправильная настройка), сбои (физические и программные атаки, атака типа «человек посередине», помехи) и несчастные случаи [24];

– модель классификации сетевых угроз Цзянь делит угрозы на сетевые по источнику угроз, сетевые по цели и сетевые по достигнутому эффекту [25];

– модель Неймана и Паркера использует восемь классов угроз: кража информации, злоупотребление ресурсами (например, по-

вреждение жесткого диска), маскировка информации, угрозы со стороны вредоносных программ, угрозы обхода аутентификации (взлом пароля), злоупотребление полномочиями (фальсификация записей), халатность или бездействие, злоупотребление вычислительными ресурсами [20].

Применяются также отраслевые подходы к классифицированию угроз [26]: так например, модель угроз RFID, включающая классификацию угроз по атакам на конкретных уровнях сетевой модели (физические, сетевые – транспортные, прикладные, стратегические и многоуровневые атаки) или модель классификации угроз веб-сервисов, предусматривающая деление по группам уязвимых программных интерфейсов (угрозы интерфейса веб-служб, угрозы системе анализа XML, угрозы вредоносного XML-контента, атаки по внешним ссылкам, подделка учетных данных XML, подделка ключа сеанса связи). Существует также классификация угроз безопасности информации для энергетических систем, включающая природные угрозы (стихийные бедствия, в том числе геомагнитные бури, землетрясения, лесные пожары, цунами, наводнение, молния, град, действия животных), случайные угрозы, преднамеренные угрозы, так называемые «возникающие» угрозы, связанные с взаимодействием энергосистемы с другими видами источников энергии.

Проведём аналогию между информационной безопасностью и безопасностью жизнедеятельности. В науке о безопасности жизнедеятельности, опасности делят по длительности негативного воздействия (переменные, периодические, постоянные), по степени завершённости процесса воздействия (реальные, потенциальные, реализованные), по мере интенсивности воздействия (допустимые, опасные, чрезвычайно опасные), по виду территории воздействия (производственные, бытовые, городские), по видам потоков, образующих воздействие (информационные энергетические, массовые), по видам источников негативного воздействия (естественные, естественно-технические, техногенные, антропогенные, антропогенно-техногенные), по размерам зоны негативного воздействия (локальные, региональные, межрегиональные, глобальные), по моменту возникновения (прогнозируемые, спонтанные), а также по воздействию на здоровье и жизнь человека [27].

Классифицирование угроз

Обобщая указанные исследования и нормы действующего законодательства, можно сформировать универсальную классификацию угроз безопасности информации, представленную на рис. 1. При разработке классификации учитывались базовые универсальные принципы классифицирования [8]:

1. Систематизация классификационных объектов, обобщающая угрозы безопасности информации для дальнейшего выявления актуальных угроз и проведения работ по их нейтрализации.

2. Представление угрозы безопасности информации в компактном виде путём выделения наиболее существенных, весомых информационных сущностей.

3. Учет психофизических ограничений восприятия информации человеком при систематизации угрозы безопасности информации – не более 7 – 8 информационных сущностей на каждом уровне классификации.

4. Интеграция и дифференциация при развитии системы классификации угрозы безопасности информации – возможность усложнения структуры классификационной системы и постепенное увеличение глубины классификации.

Классификация относится к формальному или искусственному виду классификации [28]. Некоторые дочерние объекты классификации не входят в материнские, например, природные угрозы не могут являться внутренними угрозами, не связаны с программным дестабилизирующим воздействием и не несут угрозу искажения, подделки или модификации защищаемых данных.

Определение актуальных угроз с использованием предложенной классификации основывается на презумпции опасности каждого класса угроз для конкретной информационной системы. Эксперт доказывает, какие из классов угроз требуется исключить. Доказательство строится на обосновании невозможности применения конкретного класса угрозы для конкретной информационной системы. Таким образом, предварительная классификация всего многообразия угроз безопасности информации позволяет оптимизировать работу эксперта путём исключения отдельных классов угроз из разрабатываемой модели. Этот подход не требует анализа каждой известной угрозы, что сокращает объём модели угроз и время, затрачиваемое на её подготовку.

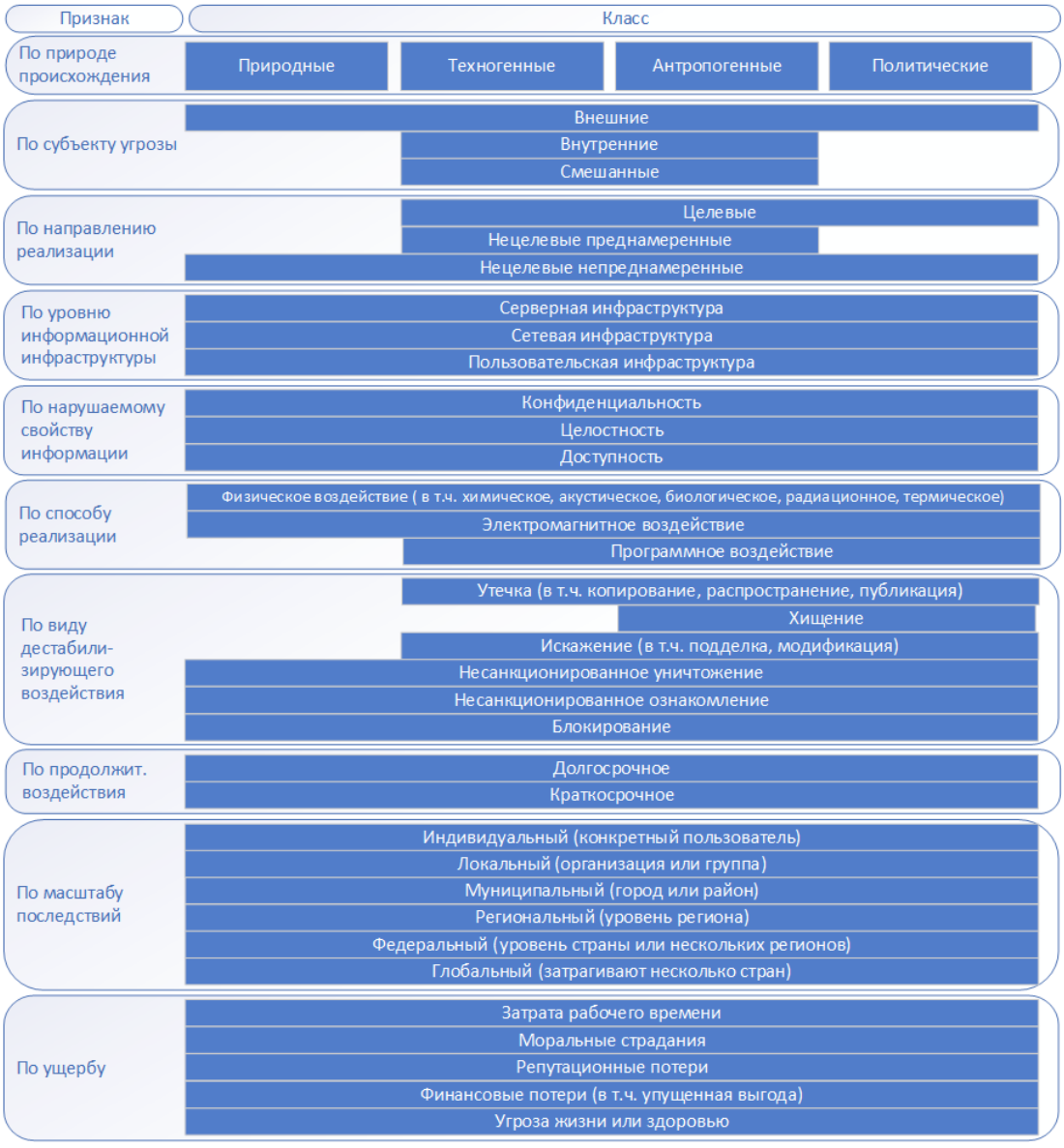

Рис. 1. Классификационная структура угроз безопасности информации. Применение универсальной классификации

Применение классификации позволяет сделать вывод об уровне риска при реализации конкретной угрозы. Расчёт уровня риска R осуществляется на основании вероятности его реализации V и оценки последствий реализации угрозы в баллах Z по предложенной классификации. Расчет уровня риска осуществляется по формуле:

$$R = V \times Z$$

Риск реализации угрозы безопасности информации тем выше, чем в больше количество классов она включена. Значение баллов последствий реализации отдельного класса угроз может быть установлено специалистом-экспертом в диапазоне от 0.1 до 1, в зависимости от тяжести последствий. Баллы также могут быть установлены вышестоящим органом или организацией для конкретного типа информационных систем. Вероятность реализации определяется специалистом-экспертом как высокая, средняя или низкая с коэффициентами 1, 0,66 и 0,33, соответственно, или рассчитана на основе существующих статистических данных.

Далее представлены примеры расчёта уровня риска реализации 4 угроз безопасности информации для гипотетической информационной системы, размещённой в Уральском федеральном округе, с пользователями в иных субъектах Российской Федерации. Базовые значения баллов последствий реализации всех классов угроз для информацион-

ной системы определены экспертным методом и представлены в табл. 1.

Пример №1. Расчёт уровня риска уничтожения информации вследствие землетрясения.

1) Классифицируем угрозу уничтожения информации вследствие землетрясения и рассчитаем сумму баллов последствий при реализации угроз Z. Классификация приведена в таблице 2.

Таблица 1

Базовые значения баллов последствий реализации угроз всех классов

№ п.п.	Тип классификации	Подходящий класс	Балл
1	По природе происхождения	Природные	1
		Техногенные	0,8
		Антропогенные	0.9
		Политические	0,6
2	По субъекту угрозы	Внешние	0,9
		Внутренние	1
		Смешанные	0,9
3	По направлению реализации	Целевые	1
		Нецелевые преднамеренные	0,6
		Нецелевые непреднамеренные	0,2
4	По уровню информационной инфраструктуры	Серверная инфраструктура	1
		Сетевая инфраструктура	0,5
		Пользовательская инфраструктура	0,1
5	По нарушаемому свойству информации	Конфиденциальность	0,8
		Целостность	1
		Доступность	0,3
6	По способу реализации	Физическое воздействие	1
		Электромагнитное воздействие	0,7
		Программное воздействие	0,9
7	По виду дестабилизирующего воздействия	Утечка	0,8
		Хищение	0,7
		Искажение	0,9
		Несанкционированное уничтожение	1
		Несанкционированное ознакомление	0,6
		Блокирование	0,5
8	По продолжительности воздействия	Долгосрочное	1
		Краткосрочное	0,9
9	По масштабу последствий	Индивидуальный	0,1
		Локальный	0,4
		Муниципальный	0,7
		Региональный	0,8
		Федеральный	0,9
		Глобальный	1
10	По ущербу	Затраты рабочего времени	0,3
		Моральные страдания	0,2
		Репутационные потери	0,8
		Финансовые потери	0,9
		Угроза жизни или здоровью	1
	Z_{max} =		26,8

2) Определим вероятность реализации угрозы. Выборка землетрясений на Урале в границах Российской Федерации по годам [29] представлена на рис. 2.

За 40 лет с 1980 по 2019 год число лет с землетрясениями составило 19. Для оценки вероятности введём допущение – поток событий является стационарным. Определим

Таблица 2

Классификация угрозы уничтожения информации вследствие землетрясения

№ п.п.	Тип классификации	Подходящий класс	Балл
1	По природе происхождения	Природная	1
2	По субъекту угрозы	Внешняя	0,9
3	По направлению реализации	Нецелевая непреднамеренная	0,2
4	По уровню информационной инфраструктуры	Серверная	1
		Сетевая	0,5
5	По нарушаемому свойству информации	Целостность	1
		Доступность	0,3
6	По способу реализации	Физическое воздействие	1
7	По виду дестабилизирующего воздействия	Несанкционированное уничтожение	1
		Блокирование	0,9
8	По продолжительности воздействия	Долгосрочное	1
9	По масштабу последствий	Региональный	0,8
		Федеральный	0,9
		Глобальный	1
10	По ущербу	Затраты рабочего времени	0,3
		Моральные страдания	0,2
		Финансовые потери	0,9
		Угроза жизни и здоровью	1
	Z =		13,9

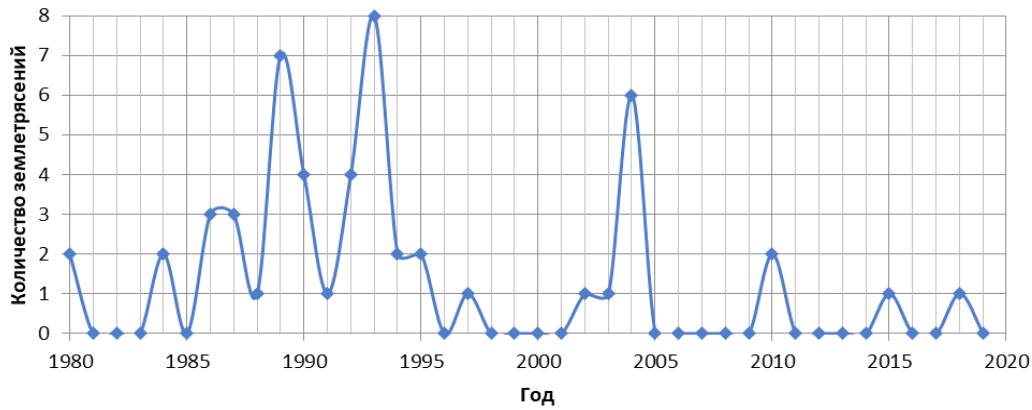

Рис. 2. Статистика землетрясений на Урале в границах Российской Федерации по годам

вероятность возникновения хотя бы одного землетрясения в течение года.

Рассчитаем среднее количество событий за 1 год (λ):

$$\lambda = \frac{p}{n} = \frac{19}{40} = 0{,}475$$

Вероятность возникновения землетрясения подчиняется распределению Пуассона. Вероятность возникновения хотя бы одного такого события в течение года определим через вероятность отсутствия землетрясений:

$$V = 1 - \frac{\lambda^m}{m!} \times e^{-\lambda} \approx 1 - \frac{0{,}475^0}{0!} \times 2{,}718^{-0{,}475} \approx 0{,}378$$

Вероятность может быть оценена, как низкая. Расчет уровня риска реализации угрозы R:

$$R = V \times Z = 0{,}378 \times 13{,}9 \approx 5{,}3$$

Уровень риска реализации угрозы ≈ 5,3 из 26,8 баллов, что составляет 19,8%.

Пример №2. Расчёт уровня риска блокирования доступа к информации вследствие выхода из строя трансформаторной подстанции, принадлежащей владельцу информационной системы.

1) Классифицируем угрозу блокирования доступа к информации вследствие выхода из строя трансформаторной подстанции, принадлежащей владельцу информационной системы и рассчитаем сумму баллов последствий при реализации угроз Z. Классификация приведена в таблице 3.

2) Определим вероятность реализации

Таблица 3

Классификация угрозы блокирования доступа к информации вследствие выхода из строя трансформаторной подстанции

№ п.п.	Тип классификации	Подходящий класс	Балл
1	По природе происхождения	Техногенная	0,8
2	По субъекту угрозы	Внутренняя	1
3	По направлению реализации	Целевая	1
		Нецелевая преднамеренная	0,6
		Нецелевая непреднамеренная	0,2
4	По уровню информационной инфраструктуры	Серверная	1
		Сетевая	0,5
5	По нарушаемому свойству информации	Доступность	0,3
6	По способу реализации	Физическое воздействие	1
7	По виду дестабилизирующего воздействия	Блокирование	0,5
8	По продолжительности воздействия	Долгосрочное	1
9	По масштабу последствий	Локальный	0,4
10	По ущербу	Затраты рабочего времени	0,3
		Финансовые потери	0,9
	Z =		9,5

угрозы. На основании статистических данных о вероятности выхода из строя трансформаторной подстанции и её технической документации ответственный специалист-эксперт делает вывод о высокой вероятности выхода из строя трансформаторной подстанции V=1.

3) Расчет уровня риска реализации угрозы R:

$$R = V \times Z = 1 \times 9,5 = 9,5$$

Уровень риска реализации угрозы R = 9,5 из 26,8 баллов, что составляет 35,5%.

Пример №3. Расчёт уровня риска несанкционированного доступа к информации вследствие применения эксплойта известной уязвимости операционной системы, установленной на сервере.

1) Классифицируем угрозу несанкционированного доступа к информации вследствие применения эксплойта известной уязвимости операционной системы, установленной на сервере и рассчитаем сумму баллов последствий при реализации угроз Z. Классификация приведена в таблице 4.

2) Определим вероятность реализации угрозы. На основании информации о наличии эксплойта, его успешного применения, а также на основании актуальности угрозы, определённой по Методике оценки уровня критичности уязвимостей программных, программно-аппаратных [30] специалист-эксперт принимает решение о высоком уровне вероятности V=1.

3) Расчет уровня риска реализации угрозы R:

$$R = V \times Z = 1 \times 16,6 = 16,6$$

Уровень риска реализации угрозы R = 16,6 из 26,8 баллов, что составляет 61,9%.

Пример №4. Расчёт уровня риска R угрозы блокирования доступа к информации вследствие прекращения поставок запасных частей, вызванного недружественными действиями иностранных государств и территорий.

1) Классифицируем угрозу блокирования доступа к информации вследствие прекращения поставок запасных частей, вызванного недружественными действиями иностранных государств и территорий, и рассчитаем сумму баллов последствий при реализации угроз Z. Классификация приведена в таблице 5.

2) Определим вероятность реализации угрозы. С учётом свершившегося события (сложная геополитическая обстановка) специалист-эксперт принимает решение о высоком уровне вероятности V=1.

3) Расчет уровня риска реализации угрозы R:

$$R = V \times Z = 1 \times 11,5 = 11,5$$

Уровень риска реализации угрозы = 11,5 из 26,8 баллов, что составляет 42,9%.

Наиболее высокий уровень риска достигается реализацией угрозы несанкционированного доступа к информации вследствие применения эксплойта известной уязвимости операционной системы, установленной на сервере. Наименьший уровень риска для конкретной территории представляет угроза уничтожения информации вследствие землетрясения.

Таблица 4

Классификация угрозы несанкционированного доступа вследствие применения эксплойта известной уязвимости операционной системы

№ п.п.	Тип классификации	Подходящий класс	Балл
1	По природе происхождения	Антропогенная	0,9
2	По субъекту угрозы	Внешняя	0,9
		Внутренняя	1
		Смешанная	0,9
3	По направлению реализации	Целевая	1
4	По уровню информационной инфраструктуры	Серверная	1
5	По нарушаемому свойству информации	Конфиденциальность	0,8
		Целостность	1
		Доступность	0,3
6	По способу реализации	Программное воздействие	0,9
7	По виду дестабилизирующего воздействия	Утечка	0,8
		Хищение	0,7
		Искажение	0,9
		Несанкционированное уничтожение	1
		Несанкционированное ознакомление	0,6
		Блокирование	0,5
8	По продолжительности воздействия	Краткосрочное	0,9
9	По масштабу последствий	Индивидуальный	0,1
		Локальный	0,4
10	По ущербу	Затраты рабочего времени	0,3
		Репутационные потери	0,8
		Финансовые потери	0,9
	Z =		16,6

Таблица 5

Классификация угрозы блокирования доступа к информации вследствие прекращения поставок запасных частей

№ п.п.	Тип классификации	Подходящий класс	Балл
1	По природе происхождения	Политическая	0,6
2	По субъекту угрозы	Внешняя	0,9
3	По направлению реализации	Нецелевая преднамеренная	0,6
4	По уровню информационной инфраструктуры	Серверная	1
		Сетевая	0,5
5	По нарушаемому свойству информации	Доступность	0,3
6	По способу реализации	Физическое воздействие	1
		Программное воздействие	0,9
7	По виду дестабилизирующего воздействия	Блокирование	0,5
8	По продолжительности воздействия	Долгосрочное	1
9	По масштабу последствий	Индивидуальный	0,1
		Локальный	0,4
		Муниципальный	0,7
		Федеральный	0,9
10	По ущербу	Затраты рабочего времени	0,3
		Репутационные потери	0,8
		Финансовые потери	1
	Z =		11,5

Риск блокирования доступа к информации вследствие выхода из строя трансформаторной подстанции, принадлежащей владельцу информационной системы, и блокирования доступа к информации вследствие прекращения поставок запасных частей, вызванного недружественными действиями иностранных государств и территорий, имеет среднее значение. При этом значение уровня рисков больше нуля, что является основанием для их учёта среди актуальных угроз в разрабатываемой модели угроз.

Заключение

Предлагаемая классификация угроз безопасности информации представляет собой универсальный источник классов угроз, позволяющий организовать их систематизированное представление и обозначить связи между ними. Применение классификации в ходе экспертной оценки при подготовке моделей угроз даёт возможность рассмотреть наиболее широкий спектр угроз безопасности информации, а также представить численную оценку рисков их реализации. Классификация может применяться в оценке угроз безопасности информации ГИС, МИС и КИИ совместно с действующей методикой оценки угроз и с учётом требований законодательства. В 2023 году классификация опробована в качестве дополнительного средства оценки угроз безопасности информации при модернизации ГИС, что позволило представить численную оценку угроз, существенно расширило спектр актуальных угроз, сократило временные затраты на разработку проекта модели. Разработанная модель угроз согласована с ФСТЭК России и находится в стадии согласования с ФСБ России.

Литература

1. Национальный стандарт РФ «ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» от 08.12.2008 № 532-ст // Каталог национальных стандартов www.rst.gov.ru. – 2008 г.

2. Национальный стандарт РФ «ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» от 15.11.2012 № N 814-ст // Каталог национальных стандартов www.rst.gov.ru. – 2012 г.

3. Банк данных угроз безопасности информации // Официальный интернет-сайт ФСТЭК России [Электронный ресурс]. – Режим доступа: URL: https://bdu.fstec.ru:8443/threat (дата обращения: 07.05.2023).

4. «Методический документ. Методика оценки угроз безопасности информации» от 05.02.2021 Официальный Интернет-сайт ФСТЭК России https://fstec.ru. – 2021 г.

5. Геологическая служба США [Электронный ресурс]. – Режим доступа: URL: https://earthquake.usgs.gov/earthquakes/map/ (дата обращения: 11.04.2023).

6. Найденов В.И., Кожевникова И.А. Почему так часто происходят наводнения? // Природа. - 2003. - №9. - С. 20-12.

7. Technological disasters // Научный центр по эпидемиологическим катастрофам Брюсселя URL: https://cred.be/sites/default/files/CC60.pdf (дата обращения: 08.04.2023).

8. Омельченко В.В. Общая теория классификации. Часть I. Основы системологии познания действительности.: - М.: ООО «ИПЦ «Маска», 2008.

9. Указ Президента Российской Федерации «Указ Президента Российской Федерации Об утверждении доктрины информационной безопасности Российской Федерации» от 05.12.2016 № 646 // Интернет-сайт Президента Российской Федерации http://kremlin.ru. – 2016 г.

10. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15.02.2008 Официальный Интернет-сайт ФСТЭК России https://fstec.ru. – 2008 г.

11. Киреенко, А. Е. Современные проблемы в области информационной безопасности: классические угрозы, методы и средства их предотвращения / А. Е. Киреенко. – Текст: непосредственный // Молодой ученый. – 2012. – № 3 (38). – С. 40-46. – [Электронный ресурс]. – Режим доступа: URL: https://moluch.ru/archive/38/4365/ (дата обращения: 07.05.2023).

12. Иванов, К. К. Угрозы безопасности информации в автоматизированных системах / К. К. Иванов, Р. Н. Юрченко, А. С. Ярмонов. – Текст: непосредственный // Молодой ученый. – 2016. – № 29 (133). – С. 20-22. – [Электронный ресурс]. – Режим доступа: URL: https://moluch.ru/archive/133/37181/ (дата обращения: 07.05.2023).

13. Алексеев Дмитрий Михайлович, Иваненко Кирилл Николаевич, Убирайло Виктор Николаевич Классификация угроз информационной безопасности // Символ науки. 2016. №9-1. [Электронный ресурс]. – Режим доступа: URL: https://cyberleninka.ru/article/n/klassifikatsiya-ugroz-informatsionnoy-bezopasnosti (дата обращения: 31.05.2023).

14. Вихорев С.В. Классификация угроз информационной безопасности // CNews. Аналитика. – 2001. [Электронный ресурс]. – Режим доступа: [Электронный ресурс]. – Режим доступа: URL: https://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml?ysclid=libnc6cv6d667276492 (дата обращения: 12.03.2023).

15. Dokuchaev V.A., Maklachkova V.V., Statev V.Yu. Classification of personal data security threats in information systems // T-Comm. 2020. №1. [Электронный ресурс]. – Режим доступа: URL: https://cyberleninka.ru/article/n/classification-of-personal-data-security-threats-in-information-systems (дата обращения: 15.03.2023).

16. Курейчик В.М., Сахарова О.Н., Пирожков С.С. УГРОЗЫ В ОБЛАСТИ ХРАНЕНИЯ ДАННЫХ // ИВД. 2021. №7 (79). [Электронный ресурс]. – Режим доступа: URL: https://cyberleninka.ru/article/n/ugrozy-v-oblasti-hraneniya-dannyh (дата обращения: 06.05.2023).

17. Alshboul Y., Wang Y., Nepali R.K. Big Data LifeCycle: Threats and Security Model // Twenty-first Americas Conference on Information Systems, Puerto Rico. 2015. [Электронный ресурс]. – Режим доступа: URL: https://www.researchgate.net/publication/281079716_Big_Data_LifeCycle_Threats_and_Security_Model (дата обращения: 23.10.2021).

18. Otuoze A. O., Mustafa M. W., Larik R. M. Smart grids security challenges: Classification by sources of threats //Journal of Electrical Systems and Information Technology. – 2018. – Т. 5. – №. 3. – С. 468-483.

19. ISO 7498-2:1989 Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture // International Organization for Standardization URL: https://www.iso.org/standard/14256.html (дата обращения: 07.05.2023).

20. Kjaerland M. A taxonomy and comparison of computer security incidents from the commercial and government sectors //Computers & Security. – 2006. – Т. 25. – №. 7. – С. 522-538.

21. Avizienis A. et al. Basic concepts and taxonomy of dependable and secure computing //IEEE transactions on dependable and secure computing. – 2004. – Т. 1. – №. 1. – С. 11-33.

22. Ruf L. et al. Threat Modeling in Security Architecture-The Nature of Threats. ISSS Working Group on Security Architectures. – 2006.

23. Farahmand F. et al. A management perspective on risk of security threats to information systems // Information Technology and Management. – 2005. – Т. 6. – С. 203-225.

24. Trivedi K. S. et al. Dependability and security models //2009 7th International Workshop on Design of Reliable Communication Networks. – IEEE, 2009. – С. 11-20.

25. Tang J. et al. A scalable architecture for classifying network security threats //Science and Technology on Information System Security Laboratory. – 2012. – С. 1-4.

26. Jouini M., Rabai L. B. A. Threats classification: state of the art //Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security. – 2016. – С. 368-392.

27. Голобокова Г. И., Викулова А. А. Подходы к классификации опасностей в дисциплине «Безопасность жизнедеятельности» //Инновационные технологии в технике и образовании. – 2020. – С. 275-284.

28. Субботин А.Л. Классификация. - М: Российская Академия Наук. Институт философии. – 2001.

29. Землетрясения на Урале (полный список) // Ураловед [Электронный ресурс]. – Режим доступа: URL: https://uraloved.ru/zemletryaseniya-na-urale-spisok (дата обращения: 03.28.2023).

30. «Методический документ. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств» от 28.11.2022 Официальный интернет-сайт ФСТЭК России https://fstec.ru. – 2022 г.

References

1. Natsional'nyy standart RF «GOST R 53114-2008 «Zashchita informatsii. Obespecheniye informatsionnoy bezopasnosti v organizatsii. Osnovnyye terminy i opredeleniya» ot 08.12.2008 № 532-st // Katalog natsional'nykh standartov www.rst.gov.ru. – 2008 g.

2. Natsional'nyy standart RF «GOST R ISO/MEK 15408-1-2012 «Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologiy. Chast' 1. Vvedeniye i obshchaya model'» ot 15.11.2012 № N 814-st // Katalog natsional'nykh standartov www.rst.gov.ru. – 2012 g.

3. Bank dannykh ugroz bezopasnosti informatsii // Ofitsial'nyy internet-sayt FSTEK Rossii [Elektronnyy resurs]. – Rezhim dostupa: URL: https://bdu.fstec.ru:8443/threat (data obrashcheniya: 07.05.2023).

4. «Metodicheskiy dokument. Metodika otsenki ugroz bezopasnosti informatsii» ot 05.02.2021 Ofitsial'nyy Internet-sayt FSTEK Rossii https://fstec.ru. – 2021 g.

5. Geologicheskaya sluzhba SSHA [Elektronnyy resurs]. – Rezhim dostupa: URL: https://earthquake.usgs.gov/earthquakes/map/ (data obrashcheniya: 11.04.2023).

6. Naydenov V.I., Kozhevnikova I.A. Pochemu tak chasto proiskhodyat navodneniya? // Priroda. - 2003. - №9. - S. 20-12.

7. Technological disasters // Nauchnyy tsentr po epidemiologicheskim katastrofam Bryusselya URL: https://cred.be/sites/default/files/CC60.pdf (data obrashcheniya: 08.04.2023).

8. Omel'chenko V.V. Obshchaya teoriya klassifikatsii. Chast' I. Osnovy sistemologii poznaniya deystvitel'nosti.: - M.: OOO «IPTS «Maska», 2008.

9. Ukaz Prezidenta Rossiyskoy Federatsii "Ukaz Prezidenta Rossiyskoy Federatsii Ob utverzhdenii doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii" ot 05.12.2016 № 646 // Internet-sayt Prezidenta Rossiyskoy Federatsii http://kremlin.ru. – 2016 g.

10. «Bazovaya model' ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh» ot 15.02.2008 Ofitsial'nyy Internet-sayt FSTEK Rossii https://fstec.ru. – 2008 g.

11. Kireyenko, A. Ye. Sovremennyye problemy v oblasti informatsionnoy bezopasnosti: klassicheskiye ugrozy, metody i sredstva ikh predotvrashcheniya / A. Ye. Kireyenko. – Tekst: neposredstvennyy // Molodoy uchenyy. – 2012. – № 3 (38). – S. 40-46. – [Elektronnyy resurs]. – Rezhim dostupa: URL: https://moluch.ru/archive/38/4365/ (data obrashcheniya: 07.05.2023).

12. Ivanov, K. K. Ugrozy bezopasnosti informatsii v avtomatizirovannykh sistemakh / K. K. Ivanov, R. N. Yurchenko, A. S. Yarmonov. – Tekst: neposredstvennyy // Molodoy uchenyy. – 2016. – № 29 (133). – S. 20-22. – [Elektronnyy resurs]. – Rezhim dostupa: URL: https://moluch.ru/archive/133/37181/ (data obrashcheniya: 07.05.2023).

13. Alekseyev Dmitriy Mikhaylovich, Ivanenko Kirill Nikolayevich, Ubiraylo Viktor Nikolayevich Klassifikatsiya ugroz informatsionnoy bezopasnosti // Simvol nauki. 2016. №9-1. [Elektronnyy resurs]. – Rezhim dostupa: URL: https://cyberleninka.ru/article/n/klassifikatsiya-ugroz-informatsionnoy-bezopasnosti (data obrashcheniya: 31.05.2023).

14. Vikhorev S.V. Klassifikatsiya ugroz informatsionnoy bezopasnosti // CNews. Analitika. – 2001. [Elektronnyy resurs]. – Rezhim dostupa: [Elektronnyy resurs]. – Rezhim dostupa: URL: https://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml?ysclid=libnc6cv6d667276492 (data obrashcheniya: 12.03.2023).

15. Dokuchaev V.A., Maklachkova V.V., Statev V.Yu. Classification of personal data security threats in information systems // T-Comm. 2020. №1. [Electronic resource]. - Mode of access: URL: https://cyberleninka.ru/article/n/classification-of-personal-data-security-threats-in-information-systems (access date: 15.03.2023).

16. Kureychik V.M., Sakharova O.N., Pirozhkov S.S. UGROZY V OBLASTI KHRANENIYA DANNYKH // IVD. 2021. №7 (79). [Elektronnyy resurs]. – Rezhim dostupa: URL: https://cyberleninka.ru/article/n/ugrozy-v-oblasti-hraneniya-dannyh (data obrashcheniya: 06.05.2023).

17. Alshboul Y., Wang Y., Nepali R.K. Big Data LifeCycle: Threats and Security Model // Twenty-first Americas Conference on Information Systems, Puerto Rico. 2015. [Electronic resource]. - Access mode: URL: https://www.researchgate.net/publication/281079716_Big_Data_LifeCycle_Threats_and_Security_Model (accessed 23.10.2021).

18. Otuoze A. O., Mustafa M. W., Larik R. M. Smart grids security challenges: Classification by sources of threats // Journal of Electrical Systems and Information Technology. - 2018. - T. 5. - №. 3. - C. 468-483.

19. ISO 7498-2:1989 Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture // International Organization for Standardization URL: https://www.iso.org/standard/14256.html (accessed 07.05.2023).

20. Kjaerland M. A taxonomy and comparison of computer security incidents from the commercial and government sectors //Computers & Security. - 2006. - T. 25. - №. 7. - C. 522-538.

21. Avizienis A. et al. Basic concepts and taxonomy of dependable and secure computing //IEEE transactions on dependable and secure computing. - 2004. - T. 1. - №. 1. - C. 11-33.

22. Ruf L. et al. Threat Modeling in Security Architecture-The Nature of Threats. ISSS Working Group on Security Architectures. - 2006.

23. Farahmand F. et al. A management perspective on risk of security threats to information systems/ Information Technology and Management. - 2005. - VOL. 6, PP. 203-225.

24. Trivedi K. S. et al. Dependability and security models //2009 7th International Workshop on Design of Reliable Communication Networks. - IEEE, 2009. - C. 11-20.

25. Tang J. et al. A scalable architecture for classifying network security threats //Science and Technology on Information System Security Laboratory. - 2012. - С. 1-4.

26. Jouini M., Rabai L. B. A. Threats classification: state of the art //Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security. - 2016. - С. 368-392.

27. Golobokova G. I., Vikulova A. A. Podkhody k klassifikatsii opasnostey v distsipline «Bezopasnost' zhiznedeyatel'nosti» //Innovatsionnyye tekhnologii v tekhnike i obrazovanii. – 2020. – S. 275-284.

28. Subbotin A.L. Klassifikatsiya. - M: Rossiyskaya Akademiya Nauk. Institut filosofii. – 2001.

29. Zemletryaseniya na Urale (polnyy spisok) // Uraloved [Elektronnyy resurs]. – Rezhim dostupa: URL: https://uraloved.ru/zemletryaseniya-na-urale-spisok (data obrashcheniya: 03.28.2023).

30. «Metodicheskiy dokument. Metodika otsenki urovnya kritichnosti uyazvimostey programmnykh, programmno-apparatnykh sredstv» ot 28.11.2022 Ofitsial'nyy internet-sayt FSTEK Rossii https://fstec.ru. – 2022 g.

ПОВЫШЕВ Александр Александрович, аспирант Федерального государственного автономного образовательного учреждения высшего образования «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, пр. Ленина, 76. E-mail: nornmail@mail.ru

POVYSHEV Aleksandr Aleksandrovich, postgraduate student of the Federal State Autonomous Educational Institution of Higher Education "South Ural State University (National Research University)". 454080, Chelyabinsk, 76 Lenin Avenue, E-mail: nornmail@mail.ru

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой «Защита информации» Федерального государственного автономного образовательного учреждения высшего образования «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, пр. Ленина, 76. E-mail: sokolovan@susu.ru

SOKOLOV Alexander Nikolaevich, PhD in Technical Sciences, Associate Professor, Head of Information Security Department, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (National Research University)". 454080, Chelyabinsk, 76 Lenin Avenue, E-mail: sokolovan@susu.ru

МИЩЕНКО Евгений Юрьевич, кандидат технических наук, преподаватель кафедры «Защита информации» Федерального государственного автономного образовательного учреждения высшего образования «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, пр. Ленина, 76. E-mail: eug6303@mail.ru

MISHCHENKO Evgeny Yuryevich, PhD in Technical Sciences, Lecturer of Information Security, Department, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (National Research University)". 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: eug6303@mail.ru