ВЫБОР НАИБОЛЕЕ ОПАСНЫХ УЯЗВИМОСТЕЙ ДЛЯ ПЕРСПЕКТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

Грызунов В.В.[1], Гришечко А.А.[2], Сипович Д.Е.[3]

***Цель** работы: определить наиболее опасные уязвимости для перспективных информационных систем критического применения (ИС КП).*

***Метод** исследования: применение метода анализа иерархий для составления иерархии альтернатив, включающих тип платформы перспективной ИС КП, аспекты информационной безопасности, типы уязвимостей. Проведение опроса экспертов с использованием балльной оценки. Преобразование результатов в матрицу парных сравнений. Получение локальных и глобальных приоритетов альтернатив.*

***Результаты** исследования: опрошены 25 экспертов разного возраста и с разным опытом работы. С точки зрения опрошенных специалистов лучшим типом платформы для перспективной распределённой информационной системы критического применения являются граничные вычисления. Доступность, аутентичность и целостность отмечены как наиболее важные аспекты информационной безопасности. Самыми опасными названы уязвимости, связанные с: 1) неполнотой проверки вводимых (входных) данных, переполнением буфера, возможностью инжекций, внедрением произвольного кода, межсайтового скриптинга, внедрения команд операционной системы и т.д.; 2) идентификацией, аутентификацией, предоставлением доступа и повышением привилегий; 3) неправильной настройкой параметров программного обеспечения, управлением ресурсами системы, получением доступа к служебной информации. Менее опасны уязвимости, использующие работоспособность аппаратного обеспечения и снижающие его устойчивость к действиям технических средств разведки и радиоэлектронной борьбы. Результаты могут использоваться для приоритезации закупок средств защиты информации, для актуализации нормативной базы регуляторов и учебных программ по подготовке специалистов информационной безопасности.*

***Ключевые слова:** граничные вычисления, туманные вычисления, облачные вычисления, информационная безопасность, распределённая информационная система, экспертные оценки.*

DOI:10.21681/2311-3456-2022-1-66-75

Введение

Развитие информационных систем критического применения опережает изменение нормативных документов регуляторов и учебные программы ВУЗов.

Информационные системы критического применения (ИС КП) являются основой объектов критически важной информационной инфраструктуры (КИИ) и должны быть защищены согласно классу объекта КИИ[4]. В основе создания системы защиты ИС КП лежит модель угроз. По результатам описания угроз формируются требования к защите информации[5]. Модель угроз строится на анализе уязвимостей ИС КП.

С другой стороны ИС КП имеют тенденцию к распределению в пространстве-времени и построению с использованием технологий облачных, туманных и граничных вычислений [1]. Очевидно, что для каждого варианта построения ИС КП характерны свои уязвимости.

Цель исследования – определить наиболее опасные уязвимости для перспективных ИС КП.

Под уязвимостью понимается недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации[6].

4 Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

5 п.13.3 Приказа ФСТЭК от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

6 ГОСТР 56546— 2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем

1 Грызунов Виталий Владимирович, кандидат технических наук, доцент кафедры информационных технологий и систем безопасности Российского государственного гидрометеорологического университета, г. Санкт-Петербург, Россия. ORCID 0000-0003-4866-217X. E-mail: viv1313r@mail.ru

2 Гришечко Анна Андреевна, студент Петербургского государственного университета путей сообщений императора Александра I, г. Санкт-Петербург, Россия. ORCID 0000-0002-3578-5958. E-mail: mlngaa25@gmail.com

3 Сипович Дмитрий Евгеньевич, старший преподаватель кафедры информационных технологий и систем безопасности Российского государственного гидрометеорологического университета, г. Санкт-Петербург, Россия. ORCID 0000-0003-4681-6606. E-mail: Sipovich@electronic.spb.ru

Существующие подходы анализа уязвимостей и угроз направлены, в основном, на решение частных задач. И это отчасти оправдано, потому что каждая информационная система в чём-то уникальна.

Обзор существующих исследований

В статье [2] исследуются угрозы на разработки программного обеспечения (SDLC) с использованием классификации угроз, основанной на рисках. Результаты предлагаемого метода сравниваются с результатами Microsoft stride[7] для определения границ компонентов, ранжирования атак и лучшего понимания угроз разработки и эксплуатации программного обеспечения в процессе разработки программного обеспечения. Подход позволяет работать с угрозами и уязвимостями конкретной проектируемой системы, но не позволяет оценить уязвимости системы как таковой.

В работе [3] рассмотрен подход к построению модели угроз, при использовании метода объектно-ориентированного проектирования. Данный метод использует UML-диаграммы при описании концептуальной модели угроз информационной безопасности, способов реализации угроз, сценариев реализации угрозы и сценариев защиты.

Используемая методология проектирования является полезным инструментом в разработке проекта системы информационной безопасности и модели угроз безопасности, однако данный метод позволяет получить только качественное представление об угрозах и уязвимостях, поэтому их невозможно ранжировать по степени опасности.

Авторы в [4] представили метод кластерного анализа при исследовании пространственно-временной модели угроз автоматизированной системы управления технологическим процессом (АСУ ТП). При использовании данного метода получено систематизированное множество частных моделей угроз для подсистем АСУ ТП. Однако авторы не конкретизируют способы получения множества уязвимостей и угроз.

В исследовании [5] описана методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining. Она основана на построении семантической модели дескрипторов безопасности с целью автоматизации низкоуровневого моделирования сценариев реализации угроз на основе описания шаблонов компьютерных атак (CAPEC, ATT&CK, OWASP, STIX, WASC и др). Для префильтрации несвязанных или недостижимых вершин при выполнении основных этапов анализа согласно методике ФСТЭК России. Метод имеет ограниченное применение при работе с ранее неизвестными уязвимостями и оценивании ИС КП как таковой.

Работа [6] сосредоточена в основном на изучении потенциала нарушителя и предлагает анализировать угрозы всех уровней АСУ ТП на основе теоретико-игровой модели Штакельберга.

В статье [7] предлагается использовать набор взвешенных критериев, при котором инженер по безопасности устанавливает веса на основе организационных приоритетов и ограничений. Это подходит для уже существующего или проектируемого конкретного экземпляра ИС.

Авторы в [7] анализируют возможности уязвимостей и угроз путём создания «графа соединений», связывающего уязвимости, пользователей, устройства и т.д. Делается упор на распределённом характере уязвимостей. Однако в итоге получается только качественная оценка, и ничего не говорится о том, как именно данные об уязвимостях попадают на граф.

Наиболее близкими к настоящей работе являются исследование [9], в котором авторы опираются на стандарт ISO/IEC 27002:2005 и используют метод анализа иерархий для получения общей оценки безопасности. И исследование [10], где анализируются уязвимости на основе ISO/IEC 27001:2013, используется нечёткость при построении иерархии приоритетов системы управления информационной безопасностью для облачных и граничных информационных систем. Однако авторы рассматривают не первоисточники проблем информационной безопасности (уязвимости), а применяемые средства защиты. Это подразумевает синтез системы защиты путём перебора всех возможных вариантов. Особо хочется отметить тот момент, что авторы не оценили трудоёмкость работы экспертов по ранжированию альтернатив, и никак не попытались её снизить. Это обстоятельство увеличивает риск не выполнить исследование из-за человеческого фактора.

Для достижения цели настоящего исследования необходимо улучшить подходы, предложенные в работах [9, 10] в части задания иерархии и упрощения создания матриц парных сравнений.

Метод исследования

Метод анализа иерархий (МАИ) позволяет декомпозировать сложные проблемы на более простые и выстроить иерархию альтернатив на основе количественных оценок [11].

Этапы классического МАИ:

1. выбрать цель исследования;
2. провести декомпозицию цели и сформировать её иерархию;
3. рассчитать локальные приоритеты альтернатив на каждом уровне иерархии;
4. рассчитать глобальные приоритеты альтернатив.

При проведении исследование предполагалось, что будущие ИС КП будут распределены в пространстве-времени.

ИС КП рассматривалась как система управления с неопределённостью своей структуры, решаемых задач и воздействия среды [12]. Иерархия, по которой оценивались уязвимости, представлена на рис. 1.

На первом уровне иерархии рассматриваются варианты построения распределённой ИС КП на основе всех современных распределённых типов платформ:

7 Угрозы, входящие в средство моделирования угроз (Майкрософт) https://docs.microsoft.com/ru-ru/azure/security/develop/threat-modeling-tool-threats

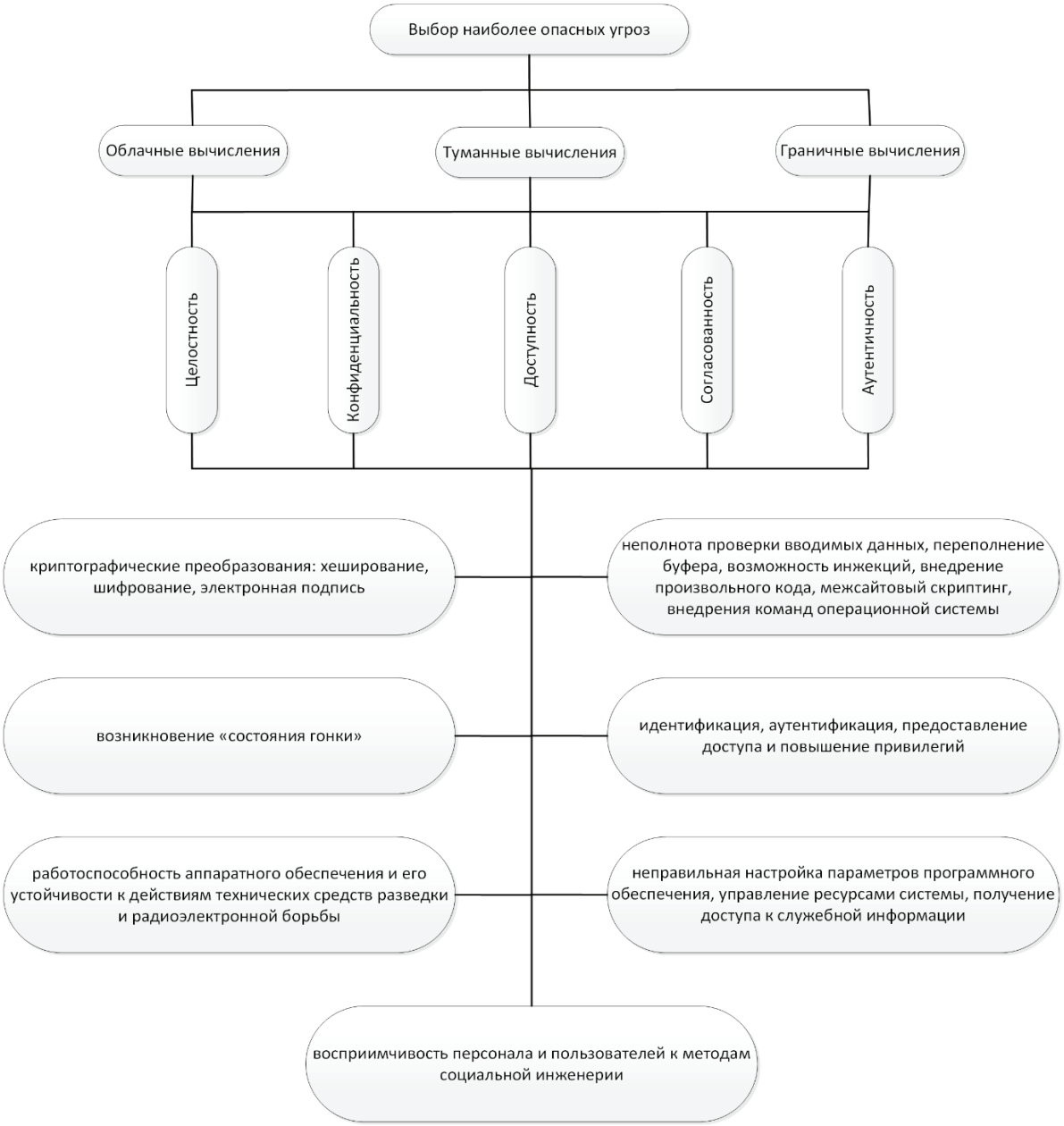

Рис. 1. Иерархия для изучения опасности уязвимостей ИС КП

1. облачные (cloud computing): хранение и обработка данных в центрах обработки данных, кластерных, выделенных серверах. Находятся дальше всех от пользователя;
2. туманные (fog computing): хранение и обработка данных между конечным устройством и облаком (локальные серверы, витринные базы данных, маршрутизаторы и пр.). Ближе к пользователю, чем облака, и дальше, чем граничные вычисления;
3. граничные (edge computing): обработка данных на конечных устройствах (датчики, IoT, мобильные телефоны и т.д.). Находятся ближе всех к пользователю.

Указанные номера типов платформ используются в статье в дальнейшем.

Второй уровень иерархии включает в себя следующие аспекты информационной безопасности:

1. целостность (integrity) – гарантия того, что данные не были изменены при выполнении какой-либо операции;
2. конфиденциальность (confidentiality): предоставление данных только тем пользователям и процессам, которые имеют разрешение;
3. доступность (availability): доступ к данным и связанным с ними активами авторизованным пользователям по мере необходимости;
4. аутентичность (authenticity) – свойство, гаранти-

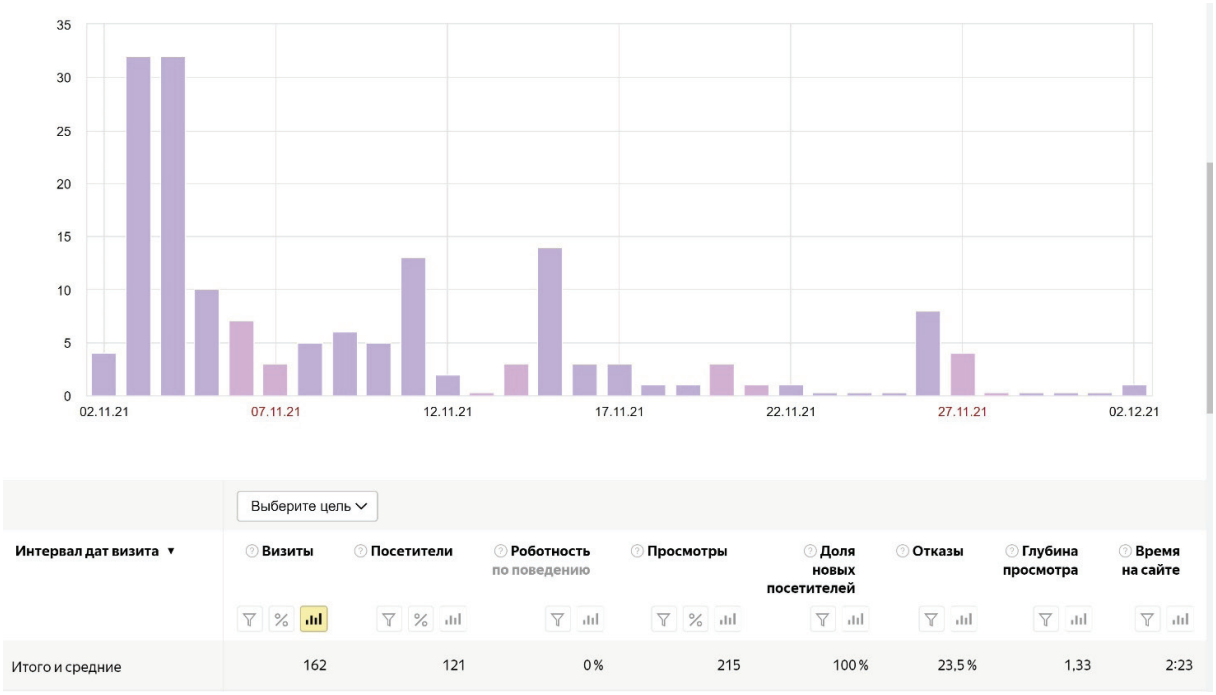

Рис. 2. Данные Яндекс-метрики заполнения анкеты

рующее, что субъект или ресурс идентичны заявленным;

5. согласованность (consistency) данных друг с другом, а также внутренняя непротиворечивость. То есть возможность из любого места системы прочитать то, что записали.

Указанные номера аспектов используются в статье в дальнейшем.

На третьем уровне иерархии располагаются уязвимости. При исследовании уязвимостей за основу взят ГОСТ 56546-2015[8], дополненный уязвимостями персонала и аппаратного обеспечения, согласно иерархической модели FIST [13]. Итоговый набор групп уязвимостей включает в себя уязвимости, связанные с:

1. неправильной настройкой параметров программного обеспечения, управлением ресурсами системы, получением доступа к служебной информации.
2. неполнотой проверки вводимых (входных) данных, переполнением буфера, возможностью инжекций, внедрением произвольного кода, межсайтового скриптинга, внедрения команд операционной системы и т.д.
3. идентификацией, аутентификацией, предоставлением доступа и повышением привилегий.
4. криптографическими преобразованиями: хеширование, шифрование, электронная подпись.
5. возникновением «состояния гонки» («состояние гонки» ошибка проектирования многопоточной системы или приложения, при которой функционирование системы или приложения зависит от порядка выполнения части кода).
6. восприимчивостью персонала и пользователей методам социальной инженерии.
7. работоспособностью аппаратного обеспечения и его устойчивости к действиям технических средств разведки и радиоэлектронной борьбы.

Указанные номера групп уязвимостей используются в дальнейшем в статье.

Классический МАИ предполагает парное сравнение и построение матрицы для каждого уровня иерархии:

$$A = a_{i,j}, a_{i,j} = w_i / w_j \ , \qquad (1)$$

где w – вес элемента в иерархии.

Поскольку вопросов получилось очень много, то было выдвинуто предположение, что проводить парное сравнение в чистом виде нецелесообразно, потому что независимые эксперты не готовы тратить много времени на прохождение опроса. Либо готовы, но к концу опроса они устанут и не будут отвечать на вопросы внимательно и вдумчиво. Это предположение подтвердилось в ходе опроса: из 121 уникальных посетителей, только 25 специалистов ответили на все поставленные вопросы и отправили анкету, т.е., примерно 21% (см. данные Яндекс-метрики на рис.2).

Для сокращения количества вопросов классический МАИ был модифицирован. Вместо парного сравнения использовалась балльная оценка каждого критерия от 1 (самая низкая оценка) до 10 (самая высокая оценка): $w_i \in [1;10]$. Классическая матрица парных сравнений составлялась на основе балльных оценок по следующей формуле:

8 ГОСТР 56546— 2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем

Рис. 3 Состав участников опроса

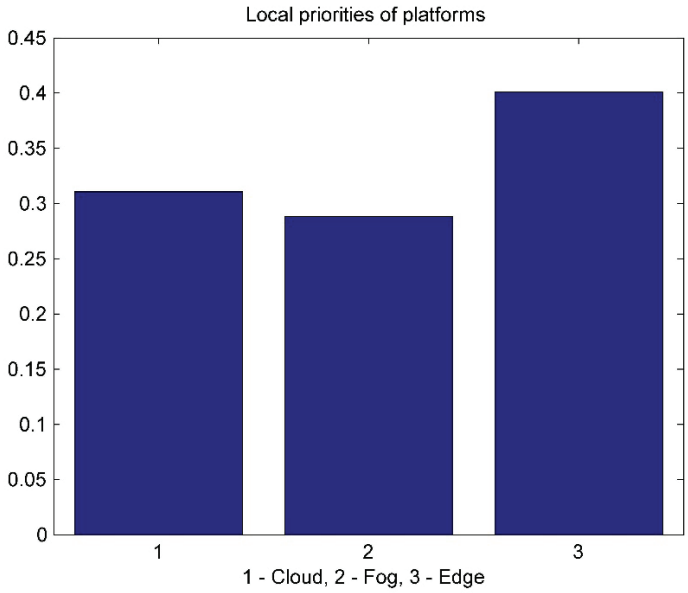

Рис. 4. Локальные приоритеты платформ, наиболее подходящих для ИС КП 1 – облачные вычисления, 2 – туманные, 3 – граничные.

$$a_{i,j} = \begin{cases} w_i - w_j + 1, w_i \geq w_j \\ 1/\left(w_i - w_j + 1\right), w_i < w_j \end{cases} . \quad (2)$$

Если w_i=w_j, то есть альтернативы равнозначны, то в матрицу попадает $a_{i,j}$=1.

В классическом применении МАИ используется шкала от 1 до 9, в опросе сделан более привычный для человека вид от 1 до 10. После чего шкала была сжата до интервала 1-9 с помощью коэффициента 0,9.

Согласно «Методике оценки угроз безопасности информации ФСТЭК»[9] при оценивании мнений экспертов максимальные и минимальные значения необходимо отбросить и после этого считать итоговое среднее значение. Однако описываемый в статье опрос характерен тем, что для некоторых альтернатив максимальные или минимальные значения указывали 28-78% экспертов. Следовательно, отбрасывать крайние значения было нецелесообразно.

Среднее значение мнений экспертов, попадающее в матрицу сравнений, может определяться двумя способами:

1. посчитать среднее значение проставленных баллов $w_i = \left(w_i^1 + w_i^2 + \ldots + w_i^K\right)/K$, потом подставить средние значения в выражение (2), где K – число экспертов;

$$a_{i,j} = \frac{\left(w_i^1 + w_i^2 + \cdots + w_i^K\right)}{K} - \frac{\left(w_j^1 + w_j^2 + \cdots + w_j^K\right)}{K} + 1 \quad (3)$$

1. подставить мнение каждого эксперта в выражение (2) и затем подсчитать среднее значение

9 Приложение 2. «Методический документ. Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021)

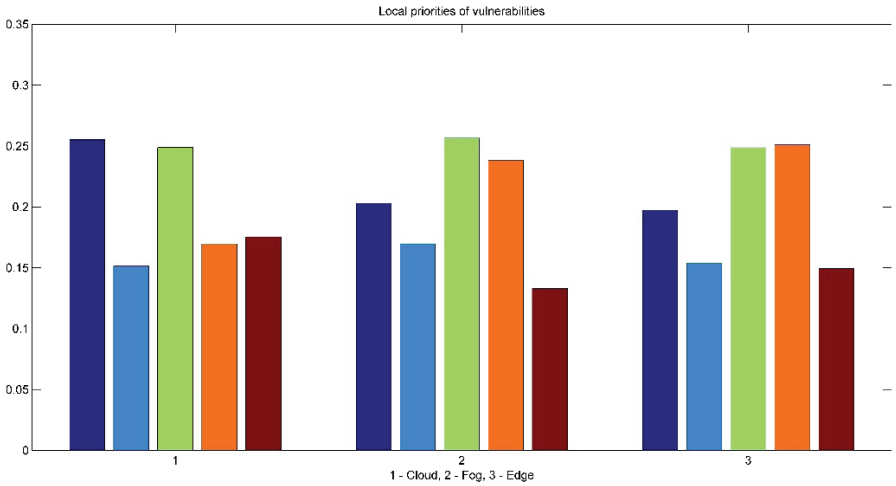

Рис.5. Локальные приоритеты аспектов информационной безопасности слева направо: целостность, конфиденциальность, доступность, аутентичность, согласованность

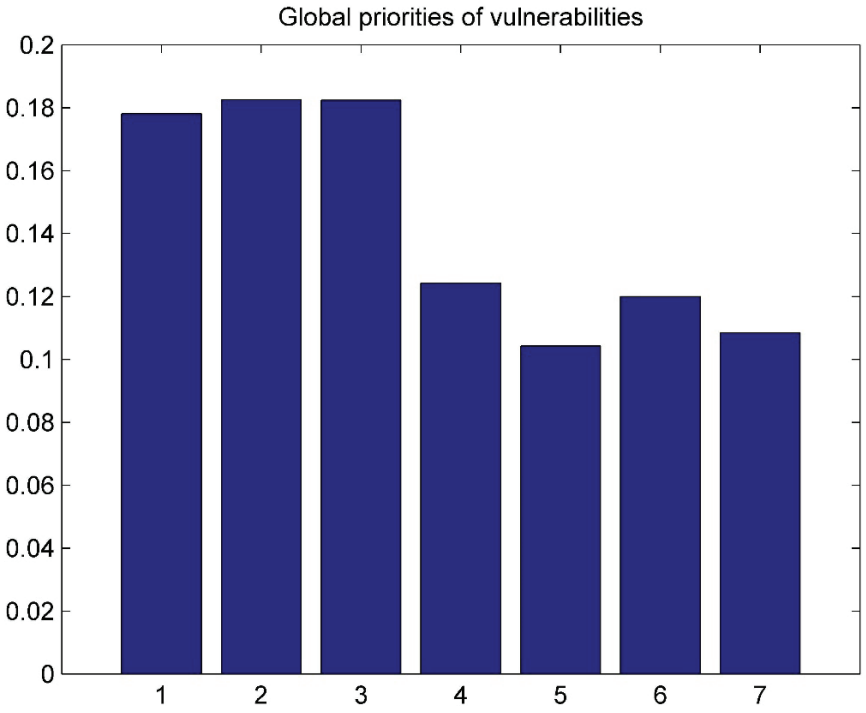

Рис. 6. Глобальные приоритеты уязвимостей (номер группы уязвимости описан выше)

$$\frac{\left(w_i^1 - w_j^1 + 1\right) + \ldots + \left(w_i^K - w_j^K + 1\right)}{K} = \\ = \frac{\left(w_i^1 + \ldots + w_i^K\right) - \left(w_j^1 + w_j^K\right) + K}{K} = \\ = \frac{\left(w_i^1 + w_i^2 + \ldots + w_i^K\right)}{K} - \frac{\left(w_j^1 + w_j^2 + \ldots + w_j^K\right)}{K} + 1 \quad (4)$$

Как видно из преобразований, оба пути ведут к одному результату, поэтому их выбор не имеет значения.

Оценки всех экспертов имели одинаковый вес, потому что более опытные эксперты знают в деталях работу уже существующих систем, но могут иметь «замыленный» взгляд. Более молодые эксперты (21-29 лет) не так хорошо знают существующие системы, но могут непредвзято оценивать нововведения и тренды. Влияние молодых экспертов на результат снизи-

лось автоматически, потому что таких экспертов было всего 26,9% (см. рис.3).

Анкета составлена с использованием Яндекс-форм, доступна по адресам в Интернет и может использоваться для более масштабных исследований:

https://vk.cc/c8qNI8 (русская версия)

https://vk.cc/c8qNKs (английская версия)

Приглашаем специалистов внести свой вклад в развитие безопасности.

Обработка результатов производилась с помощью программы, написанной на языке Матлаб.

Результат исследования

Анкета рассылалась только специалистам информационной безопасности. Описание участников приведено на рис. 3.

В опросе принимали участие эксперты с разным опытом и разного возраста. Как видно из рисунка 50% опрошенных имеют опыт работы по специальности больше 8 лет, 30,8% опрошенных младше 30 лет.

Интересно, что наиболее подходящей платформой для ИС КП эксперты отметили граничные вычисления (см. рис. 4), которые никак не отражены в настоящий момент в руководящих документах ФСТЭК и программах высших учебных заведений, готовящих специалистов информационной безопасности.

Локальные приоритеты аспектов информационной безопасности для каждого типа платформы ИС КП приведены на рис. 5.

Для граничных и туманных платформ ИС КП наиболее важными считаются доступность и аутентичность, а для облачных вычислений – целостность и доступность.

Глобальные приоритеты уязвимостей ИС КП располагаются так, как показано на рис. 6.

Из рис. 6 видно, что эксперты больше всего обеспокоены уязвимостями, связанными с:

- неполнотой проверки вводимых (входных) данных, переполнением буфера, возможностью инжекций, внедрением произвольного кода, межсайтового скриптинга, внедрения команд операционной системы и т.д.
- идентификацией, аутентификацией, предоставлением доступа и повышением привилегий;
- неправильной настройкой параметров программного обеспечения, управлением ресурсами системы, получением доступа к служебной информации.

И меньше всего:

- возникновением «состояния гонки» («состояние гонки» ошибка проектирования многопоточной системы или приложения, при которой функционирование системы или приложения зависит от порядка выполнения части кода).
- работоспособностью аппаратного обеспечения и его устойчивостью к действиям технических средств разведки и радиоэлектронной борьбы.

Обсуждение результатов

В п.2.11 Методики ФСТЭК[10] предполагается, что ИС КП строится централизованно или на базе облачных вычислений, то есть туманные и граничные вычисления даже не рассматриваются как варианты для создания ИС КП. Однако согласно опросу экспертов, именно граничные вычисления являются наиболее перспективными для ИС КП. И поскольку для ИС КП характерно функционирование в агрессивной среде [14], применение распределённых вычислений для создания ИС КП требует разработки специальных методов управления ресурсами и задачами ИС, например, как это сделано в работах [15, 16].

Расставленные приоритеты, вероятно, объясняются распределённой в пространстве-времени природой ИС КП. Действительно, чем больше распределена и децентрализована система, тем актуальнее вопросы формирования периметра ИС КП, доступа пользователей в периметр, предоставления ресурсов.

И та же особенность распределения в пространстве-времени затрудняет использование уязвимостей 5 и 7 групп, что делает их не такими значимыми, как уязвимости 1-3.

Практическое применение

Результаты исследования могут войти в руководящие документы ФСТЭК и ФСБ, регулирующие безопасность перспективных объектов КИИ и их ИС, построенных на базе граничных и туманных вычислений.

Ещё один вариант использования результатов – применение при разработке учебных программ для специалистов информационной безопасности в высших учебных заведениях и соответствующих курсах повышения квалификации. В учебных программах необходимо сосредоточиться в первую очередь на безопасном программировании и способах верификации программного обеспечения, на методах и средствах аутентификации и идентификации в распределённых ИС КП, на верификации политик разграничения доступа, системном администрировании.

При построении системы защиты ИС КП в условиях ограниченного бюджета и времени можно использовать результаты данного исследования и решить, каким уязвимостям и средствам защиты уделять время и деньги в первую очередь.

Подход и программное обеспечение, описанные в данном исследовании, могут послужить началом более масштабного исследования, проводимого регуляторами на базе сформированных рабочих групп из специалистов информационной безопасности.

Адекватность полученных результатов подтверждается корректным использованием МАИ, случайной выборкой экспертов в сфере информационной безопасности из разных городов и организаций, разного возраста и разного опыта работы по специальности.

В дальнейшем предполагается проверить гипотезу

10 п.2.11 «Методический документ. Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021)

об эффективности карт Кохонена для выделения страт в выборке экспертов.

Заключение

Уязвимости перспективных ИС КП могут быть исследованы методом анализа иерархий (МАИ). Иерархия, описанная в статье, включает в себя 3 уровня:

- уровень типов платформ;
- уровень аспектов информационной безопасности;
- уровень уязвимостей.

При проведении опроса экспертов необходимое количество вопросов сокращено за счёт модификации МАИ и использовании балльной оценки.

Для создания ИС КП наиболее подходит платформа, построенная на базе граничных вычислений. Для граничных и туманных вычислений ИС КП самими важными считаются доступность и аутентичность, а для облачных вычислений доступность и целостность.

Наиболее опасными уязвимостями для ИС КП являются уязвимости, связанные с неполнотой проверки данных и внедрением произвольного кода, с идентификацией, аутентификацией и предоставлением доступа, неправильной настройкой программного обеспечения.

Описанный подход и программное обеспечение могут применяться ВУЗами при подготовке специалистов и для более масштабных исследований ФСТЭК и ФСБ.

Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) Проект №08/2020.

Литература

1. Бурлов В. Г., Грызунов В. В., Сипович Д. Е. Адаптивное управление доступностью в геоинформационной системе, использующей туманные вычисления // International Journal of Open Information Technologies. 2021. Т. 9. № 9. С. 74—87.
2. Viswanathan G., Jayagopal P. A Threat Categorization of Risk-Based approach for analyzing Security Threats early phase in SDLC // Arabian Journal for Science and Engineering. 2021. С. 1—13. DOI: 10.1007/s13369-021-05602-x.
3. Грибанова-Подкина М. Ю. Построение модели угроз информационной безопасности информационной системы с использованием методологии объектно-ориентированного проектирования //Вопросы безопасности. 2017. №. 2. DOI: 10.7256/2409-7543.2017.2.22065.
4. Абрамова Т. В., Аралбаев Т. З. Анализ пространственно-временной модели угроз для распределенной автоматизированной системы управления процессом транспортировки нефтегазового сырья //Вестник Уфимского государственного авиационного технического университета. 2020. Т. 24. №. 1 (87). С. 76—84.
5. Васильев В. И. и др. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining //Системы управления, связи и безопасности. 2021. №. 3. С. 110—134.
6. Чернов Д. В., Сычугов А. А. Формализованное представление модели угроз информационной безопасности АСУ ТП //Радиотехника. 2019. Т. 83. №. 6. С. 74—80. DOI: 10.18127/j00338486-201906(7)-13.
7. Llansó T., McNeil M., Noteboom C. Multi-criteria selection of capability-based cybersecurity solutions //Proceedings of the 52nd Hawaii International Conference on System Sciences. 2019. DOI: 10.24251/HICSS.2019.879.
8. Hadarics K. et al. Improving distributed vulnerability assessment model of cybersecurity //Central and Eastern European eDem and eGov Days. 2018. Т. 331. С. 385—393. DOI: 10.24989/ocg.v331.32.
9. Breier J., Hudec L. New approach in information system security evaluation //2012 IEEE First AESS European Conference on Satellite Telecommunications (ESTEL). IEEE, 2012. С. 1—6. DOI: 10.1109/ESTEL.2012.6400145.
10. Tariq M. I. et al. Prioritization of information security controls through fuzzy AHP for cloud computing networks and wireless sensor networks //Sensors. 2020. Т. 20. №. 5. С. 1310. DOI: 10.3390/s20051310.
11. Saaty T. L. Decision making with the analytic hierarchy process //International journal of services sciences. 2008. Т. 1. №. 1. С. 83—98. DOI:10.1504/IJSSCI.2008.017590.
12. Грызунов В. В. Концептуальная модель адаптивного управления геоинформационной системой в условиях дестабилизации // Проблемы информационной безопасности. Компьютерные системы. 2021. № 1(45). С. 102—108.
13. Грызунов В. В. Модель геоинформационной системы FIST, использующей туманные вычисления в условиях дестабилизации //Вестник Дагестанского государственного технического университета. Технические науки. 2021. Т. 48. №. 1. С. 76—89. DOI: 10.21822/2073-6185-2021-48-1-76-89.14. Burlov V. G., Gryzunov V. V., Tatarnikova T. M. Threats of information security in the application of GIS in the interests of the digital economy //Journal of Physics: Conference Series. IOP Publishing. 2020. Т. 1703. №. 1. С. 012023. DOI:10.1088/1742-6596/1703/1/012023.
14. Грызунов В. В. Метод динамического формирования пулов в информационно-вычислительных системах военного назначения // Информационно-управляющие системы. 2015. №. 1 (74). DOI; 10.15217/issn1684-8853.2015.1.13.
15. Грызунов В. В. Методика решения измерительных и вычислительных задач в условиях деградации информационно-вычислительной системы //Вестник СибГУТИ. 2015. №. 1. С. 35—46.

SELECTING THE MOST DANGEROUS VULNERABILITIES FOR PROSPECTIVE INFORMATION SYSTEMS FOR CRITICAL APPLICATIONS

GryzunovV.V.[11], Grishechko A.A.[12], Sipovich D.E.[13]

Abstract

The development of information systems of critical application is ahead of changes in regulatory documents of regulators and educational programs of universities.

Purpose of work: *to determine the most dangerous vulnerabilities for promising information systems of critical application (IS CA).*

Research method: *application of the analysis hierarcihes method to compile a hierarchy of alternatives, including the type of platform for a promising IS CA, aspects of information security, types of vulnerabilities. Conducting a survey of experts using a point assessment. Converting results to a matrix of pairwise comparisons. Getting local and global priorities of alternatives.*

Result of the study: *25 experts of different ages and with different work experience were interviewed. From the point of view of the interviewed specialists, the best type of platform for a prospective distributed information system of critical application is edge computing. Availability, authenticity and integrity are highlighted as the most important aspects of information security. The most dangerous are the vulnerabilities associated with: 1) incomplete verification of input (input) data, buffer overflow, the possibility of injections, injection of arbitrary code, cross-site scripting, injection of operating system commands, etc.; 2) identification, authentication, granting access and privilege escalation; 3) incorrect configuration of software parameters, management of system resources, access to service information. Less dangerous are vulnerabilities that use the health of hardware and reduce its resistance to the actions of technical means of reconnaissance and electronic warfare. The results can be used to prioritize the procurement of information security products, to update the regulatory framework of regulators and training programs for training information security specialists.*

Keywords: *edge computing, fog computing, cloud computing, information security, distributed information system, expert assessments.*

The reported study was funded by Russian Ministry of Science (information security), project № 08/2020.

References:

1. Burlov V. G., Gry'zunov V. V., Sipovich D. E. Adaptivnoe upravlenie dostupnost'yu v geoinformacionnoj sisteme, ispol'zuyushhej tumanny'e vy'chisleniya // International Journal of Open Information Technologies. 2021. T. 9. № 9. S. 74—87.
2. Viswanathan G., Jayagopal P. A Threat Categorization of Risk-Based approach for analyzing Security Threats early phase in SDLC // Arabian Journal for Science and Engineering. 2021. S. 1—13. DOI: 10.1007/s13369-021-05602-x.
3. Gribanova-Podkina M. Yu. Postroenie modeli ugroz informacionnoj bezopasnosti informacionnoj sistemy' s ispol'zovaniem metodologii ob"ektno-orientirovannogo proektirovaniya //Voprosy' bezopasnosti. 2017. №. 2. DOI: 10.7256/2409-7543.2017.2.22065.
4. Abramova T. V., Aralbaev T. Z. Analiz prostranstvenno-vremennoj modeli ugroz dlya raspredelennoj avtomatizirovannoj sistemy' upravleniya processom transportirovki neftegazovogo sy'r'ya //Vestnik Ufimskogo gosudarstvennogo aviacionnogo texnicheskogo universiteta. 2020. T. 24. №. 1 (87). S. 76—84.
5. Vasil'ev V. I. i dr. Metodika ocenki aktual'ny'x ugroz i uyazvimostej na osnove texnologij kognitivnogo modelirovaniya i Text Mining // Sistemy' upravleniya, svyazi i bezopasnosti. 2021. №. 3. S. 110—134.
6. Chernov D. V., Sy'chugov A. A. Formalizovannoe predstavlenie modeli ugroz informacionnoj bezopasnosti ASU TP //Radiotexnika. 2019. T. 83. №. 6. S. 74—80. DOI: 10.18127/j00338486-201906(7)-13.
7. Llansó T., McNeil M., Noteboom C. Multi-criteria selection of capability-based cybersecurity solutions //Proceedings of the 52nd Hawaii

11 Vitaliy V. Gryzunov, Ph.D. (in Tech.), Associate Professor of the Department of Information Security and Safety Systems, Russian State Hydrometeorological University (RSHU), Saint Petersburg, Russia. ORCID 0000-0003-4866-217X. E-mail: viv1313r@mail.ru

12 Anna A. Grishecko, Student, Petersburg State University of Railways of Emperor Alexander I (PGUPS), Saint Petersburg, Russia. ORCID 0000-0002-3578-5958. E-mail: mlngaa25@gmal.com.

13 Dmitriy E. Sipovich, Senior Lecturer of Department of Information Security and Safety Systems, Russian State Hydrometeorological University (RSHU), Saint Petersburg, Russia. ORCID 0000-0003-4681-6606. E-mail: Sipovich@electronic.spb.ru

International Conference on System Sciences. 2019. DOI: 10.24251/HICSS.2019.879.
8. Hadarics K. et al. Improving distributed vulnerability assessment model of cybersecurity //Central and Eastern European eDem and eGov Days. 2018. T. 331. S. 385—393. DOI: 10.24989/ocg.v331.32.
9. Breier J., Hudec L. New approach in information system security evaluation //2012 IEEE First AESS European Conference on Satellite Telecommunications (ESTEL). IEEE, 2012. S. 1—6. DOI: 10.1109/ESTEL.2012.6400145.
10. Tariq M. I. et al. Prioritization of information security controls through fuzzy AHP for cloud computing networks and wireless sensor networks //Sensors. 2020. T. 20. №. 5. S. 1310. DOI: 10.3390/s20051310.
11. Saaty T. L. Decision making with the analytic hierarchy process //International journal of services sciences. 2008. T. 1. №. 1. S. 83—98. DOI:10.1504/IJSSCI.2008.017590.
12. Gry'zunov V. V. Konceptual'naya model' adaptivnogo upravleniya geoinformacionnoj sistemoj v usloviyax destabilizacii // Problemy' informacionnoj bezopasnosti. Komp'yuterny'e sistemy'. 2021. № 1(45). S. 102—108.
13. Gry'zunov V. V. Model' geoinformacionnoj sistemy' FIST, ispol'zuyushhej tumanny'e vy'chisleniya v usloviyax destabilizacii //Vestnik Dagestanskogo gosudarstvennogo texnicheskogo universiteta. Texnicheskie nauki. 2021. T. 48. №. 1. S. 76—89. DOI: 10.21822/2073-6185-2021-48-1-76-89. 14. Burlov V. G., Gryzunov V. V., Tatarnikova T. M. Threats of information security in the application of GIS in the interests of the digital economy //Journal of Physics: Conference Series. IOP Publishing. 2020. T. 1703. №. 1. S. 012023. DOI:10.1088/1742-6596/1703/1/012023.
14. Gry'zunov V. V. Metod dinamicheskogo formirovaniya pulov v informacionno-vy'chislitel'ny'x sistemax voennogo naznacheniya // Informacionno-upravlyayushhie sistemy'. 2015. №. 1 (74). DOI; 10.15217/issn1684-8853.2015.1.13.
15. Gry'zunov V. V. Metodika resheniya izmeritel'ny'x i vy'chislitel'ny'x zadach v usloviyax degradacii informacionno-vy'chislitel'noj sistemy' //Vestnik SibGUTI. 2015. №. 1. S. 35—46.