DOI:

НЕКОТОРАЯ ОЦЕНКА РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СТРУКТУР С ИСПОЛЬЗОВАНИЕМ МЕТОДА НЕЧЕТКОЙ ЛОГИКИ[1]

Козлов А.Д., Нога Н.Л.

Институт проблем управления им. В.А. Трапезникова РАН, Россия, г. Москва

ул. Профсоюзная д.65

alkozlov@ipu.ru, noga@ipu.ru

Аннотация. Приводится анализ методов качественной и количественной оценки риска информационной безопасности организаций, имеющих сложную сетевую структуру, использующих облачные технологии. Предложена методика оценки риска информационной безопасности облачных структур, основанная на методах нечеткой логики, учитывающая уровни угроз, уязвимости, потенциальный ущерб и уровень затрат.

Ключевые слова: информационная безопасность, облачные технологии, угроза, уязвимость, ущерб, риск, нечеткая логика, лингвистическая переменная, продукционные правила, управление рисками, уровень контроля информационных ресурсов.

Введение

Интенсивная цифровизация всех аспектов современной жизни порождает новые вызовы и угрозы, которые в первую очередь связаны с проблемами обеспечения информационной безопасности на всех этапах от инициирования создания информационных систем, их эксплуатации и «утилизации» данных. Без правильной оценки риска на этих этапах невозможно соблюсти паритет между требованиями экономики к ускорению обработки постоянно возрастающих массивов информации и правами юридических и физических лиц на сохранение конфиденциальности своих данных.

По данным экспертов Группы компаний InfoWatch [1] в 2019 г. число зарегистрированных утечек информации во всем мире выросло примерно на 10% по сравнению с 2018 г., скомпрометировано было более 14 млрд записей данных различных групп пользователей (персональные данные, финансовая информация). Это почти в два раза больше, чем в предыдущем году. В России число утечек за год увеличилось более чем на 40%, число скомпрометированных записей выросло примерно в шесть раз и составило порядка 170 млн. По-прежнему наибольшему риску подвергаются персональные данные. Доля скомпрометированных персональных данных составляет 75% от общего числа. Объектами атак и утечек являются как коммерческие, так и государственные компании и организации.

Для правильной оценки риска информационной безопасности важно знать, откуда исходит основная угроза изнутри или извне, от внутреннего или внешнего нарушителя. По данным InfoWatch доля утечек от внутреннего нарушителя в 2019 году несколько уменьшилась с 61% в 2018 г. (1393 утечки) до 54% (1348), при этом количество скомпрометированных данных увеличилось почти в 4 раза и достигло 9,87 млрд. записей (70% от общего количества). Из этого числа 98% данных было скомпрометировано в результате легитимного доступа сотрудников или руководства компаний.

В современных информационных системах все чаще и в большем объеме используются облачные технологии (услуги). Экономический эффект от их использования очевиден. Однако, это таит в себе дополнительные риски. В частности, сотрудники провайдера таких услуг являются потенциальными внутренними нарушителями в своей компании, но для пользователя они являются внешними. Чем больше услуг получает пользователь от провайдера, тем больше прав легитимного доступа к данным получают сотрудники провайдера, а уровень контроля со стороны владельца информационного ресурса падает.

Вот эти некоторые особенности облачных структур позволяет учесть предлагаемая авторами методика оценки риска.

1 Анализ методов оценки риска информационной безопасности

Основными целями задачи обеспечения информационной безопасности являются:

- обеспечение доступности;
- обеспечение целостности;

[1] *Работа выполнена в рамках фундаментальной темы «Модели, методы анализа и синтеза структуры и сценариев развития социально-экономических и технических систем управления, повышения их управляемости и безопасности функционирования в условиях неопределенности, структурных возмущений и чрезвычайных ситуаций» (направление №31 ПФНИ ГАН на 2013–2020 годы)*

- обеспечение конфиденциальности.

В работе [2] сформулированы повсеместно используемые две основные методики для обеспечения информационной безопасности в распределенных корпоративных информационных системах. Первая основана на проверке соответствия обязательным требованиям стандартов и нормативно-правовых документов, а также проверке защищенности всех частей системы от актуальных угроз. Вторая основана на оценке и управлении рисками информационной безопасности [3-5].

Оценка риска состоит из оценки угроз, уязвимостей и ущерба, который может возникнуть при их реализации.

Процедура анализа риска подразумевает моделирование ситуации возникновения неблагоприятных условий, учитывая всевозможные внутренние и внешние факторы, характеризующие риск как таковой.

В целях наиболее точной оценки риска рекомендуется предварительно разработать для конкретного варианта построения информационной системы **модель угроз и нарушителя.**

Модель строится с учетом современных тенденций на основе банков данных угроз и уязвимостей [6-7].

В банках данных угроз и уязвимостей информационной безопасности из более чем 200 угроз и почти 27 тысяч уязвимостей практически 30% в той ли иной степени связаны с использованием облачных технологий.

На текущий момент существует множество методик анализа и оценки рисков. Это, например, CORAS, OCTAVE, CRAMM. Какие-то из них дают количественные, какие-то качественные оценки рисков. CRAMM дает и те и другие оценки.

Основной недостаток этих методик при практическом применении – необходимость привлечения высококвалифицированных специалистов.

В работе [8] авторами была предложена методика оценки рисков, в отличие от вышеперечисленных методологий, на основе методов нечеткой логики с учетом субъективных факторов риска, позволяющая оценивать риски в условиях большой неопределенности.

Практическая реализация предполагает использование пакета Fuzzy Logic Toolbox системы Matlab [9].

Осуществление оценки и управления риском предлагается проводить по следующему алгоритму, используемому во многих работах, связанных с оценкой рисков в информационных системах.

- Проведение идентификации (или инвентаризации) активов информационной системы корпорации.
- Проведение фильтрации множества угроз информационной системе корпорации, определение перечня актуальных угроз.
- Проведение фильтрации множества уязвимостей в информационной системе и определение перечня уязвимостей, через которые могут быть реализованы угрозы.
- Проведение расчета рисков.
  - определение уровней (термов) активов, уязвимости, вероятности реализации угрозы, ущерба (лингвистическая оценка входных и выходных параметров);
  - составление продукционных правил;
  - ввод данных в нечеткую базу данных (Мамдани или Сугено);
  - получение нечеткого вывода;
  - дефазификация выходных данных, получение конкретных значений риска.
- Проведение анализа и обработки полученных рисков, выявление остаточных рисков.
- Принятие остаточных рисков.

2 Задача оценки риска информационной безопасности

В работе [8] авторы сформулировали задачу оценки риска, используя методы нечеткой логики, следующим образом.

Пусть множество входных параметров T_i ($i = 1,...,M$) соответствует уровням угроз. Множество входных параметров V_j ($j = 1,...,N$) соответствует уровням уязвимостей. А множество входных параметров D_k (k $= 1,...,K$) соответствует уровням ущерба. Значения всех этих параметров могут принимать как количественные значения в промежутке [0;1], так и качественные значения: {низкий, средний, высокий, критический}.

Необходимо найти выходной параметр R, зависящий от перечисленных входных параметров, который и определяет уровень риска.

В соответствии с представленным алгоритмом рассмотрим следующие стадии.

Идентификацию активов информационной системы предлагается проводить с помощью оценивания экспертами ценности этих активов определяемой стоимостью ущерба, наносимого рассматриваемой организации, в случае если этими активами будут утеряны основные свойства безопасности: конфиденциальность, целостность, доступность. Введем в рассмотрение лингвистическую переменную «ценность актива» и проведем экспертное оценивание каждого актива информационной системы, с целью определения ценности по каждому их вышеперечисленных свойств безопасности. Результаты оценивания предлагается расположить в табличном виде (см. Таблицу 1).

Таблица 1. Оценка ценности активов.

№ п/п	Уровень ценности	Стоимость актива (в усл. единицах)	Границы терма «Ценность актива»
1	Пренебрежимо малая	0 - 5000	0-0,20
2	Низкая	5001 - 50000	0,21-0,40
3	Средняя	50001 - 300000	0,41-0,60
4	Высокая	300001 - 1000000	0,61-0,80
5	Критически высокая	Выше 1000001	0,81-1,00

Фильтрацию множества угроз безопасности данных в информационной системе будем осуществлять с помощью дерева атак [8] и на основе анализа, при котором учитываются:

- потенциал нарушителя безопасности информации, как внутреннего, так и внешнего;
- уровень опасности множества возможных уязвимостей системы, через которые реализуются угрозы, взятых из банков данных уязвимостей;
- множество различных вариантов осуществления угроз, приведенных в банках данных угроз;
- последствия (объемов ущерба, желательно в стоимостном выражении) осуществления угроз безопасности информации в системе.

Потенциал нарушителя можно определить как:

$$(1) \qquad G = G\,(A, K, L, M),$$

где

- параметр A определяет возможность доступа нарушителей к объектам,
- параметр K определяет компетенцию, интеллектуальный потенциал нарушителя,
- параметр L определяет техническую вооруженность нарушителя,
- параметр M определяет мотивацию нарушителя.

Значения этих параметров, вернее их количественные оценки, определяются на основании ГОСТ Р ИСО/МЭК 18045-2013, ГОСТ Р ИСО/МЭК 18045-2008. В зависимости от полученных численных значений функции G дается качественная оценка потенциала нападения нарушителя информационной безопасности.

Таблица 2. Оценка воздействия.

№ п/п	Уровень воздействия	Воздействия. Описание ущерба	Границы терма «Оценка воздействия»
1	Незначительное	Незначительное воздействие. Действия по восстановлению не требуются	0-0,25
2	Среднее	Актив можно восстановить достаточно быстро	0,26-0,50
3	Серьезное	Актив требует достаточно серьезного и длительного восстановления	0,51-0,75
4	Критическое	Актив полностью разрушен и не подлежит восстановлению	0,76-1,00

Чтобы экспертно оценить последствия реализации угрозы через конкретную уязвимость введем в рассмотрение лингвистическую переменную «Оценка воздействия» (Таблица 2). Под ущербом понимается величина, зависящая от финансовых потерь, невозможности выполнения работ по контрактам организации, компрометации данных и т.п.

Оценить же **уровень опасности уязвимостей** можно используя методику оценки CVSS (Common Vulnerability Scoring System - Общая система оценки уязвимостей. Задается в пределах от 0 до 10) [10].

Таким образом, любую угрозу безопасности информации в информационной системе корпорации можно представить в виде функции [8]:

$T = T$ (потенциал нарушителя, уязвимости, вариант реализации i-ой угрозы, активы, объем ущерба).

Рассмотрим теперь лингвистическую переменную «вероятность угрозы» (или «уровень угрозы») и экспертно определим границы ее терма, увязав тем самым активы, уязвимости и угрозы (см. Таблицу 3).

Таблица 3. Вероятность реализации угрозы.

№ п/п	Уровень вероятности	Частота возникновения угрозы	Границы терма «Вероятность угрозы»
1	Низкий	Отсутствует. Для новых активов вероятность исполнения угрозы низкая	0-0,33
2	Средний	Один – два раза в год. Для новых активов вероятность исполнения угрозы средняя	0,34-0,66
3	Высокий	Больше 2-х раз в год. Для новых активов вероятность исполнения угрозы высокая	0,67-1,00

Для учета влияния особенностей использования облачных технологий и затрат на создание информационных систем по аналогии с первыми тремя таблицами дополнительно строятся Таблицы 4 и 5 и вводятся в рассмотрение лингвистические переменные по следующим критериям рисков информационной безопасности системы: «Уровень контроля информационных ресурсов» и «Затраты на создание и эксплуатацию системы». Границы термов задаются экспертным путем, например для уровня контроля информационных ресурсов, либо, например для затрат, могут рассматриваться конкретные варианты построения систем. При этом количество термов ограничивается только количеством рассматриваемых вариантов (для затрат) или максимальным количеством продукционных правил.

Таблица 4. Уровень контроля информационных ресурсов (Кс)

№ п/п	Уровень контроля	Расположение хранилища информации	Границы терма «Уровень контроля»
1	Полный	Используется частное облако	0,95-1,00
2	Высокий	Провайдер предоставляет услуги по использованию инфраструктуры (IaaS)	0,60-0,90
3	Средний	Конкретный провайдер предоставляет услуги по хранению, обработке информации и администрированию системы (SaaS)	0,40-0,75
4	Низкий	В экстерриториальном облаке	0,10-0,50

Таблица 5. Затраты на создание и эксплуатацию системы (Z)

№ п/п	Уровень затрат	Стоимость создания и эксплуатации системы в условных единицах	Границы терма «Затраты»
1	Низкий	50 – 1000	0-0,30
2	Средний	900 – 100000	0,25-0,60
3	Высокий	90000 – 550000	0,55-0,80
4	Значительный	Более 500000	0,75-1,00

Таким образом, используется последовательность таблиц, которые связывают различные элементы в процессе анализа риска. Следовательно, уровень риска можно представить в виде функции $R = R$ *(уровень угрозы, уровень уязвимости, уровень ущерба, уровень контроля информационных ресурсов, затраты на создание и эксплуатацию системы)* или

$$(2) \qquad R = R\,(p(V), p(T), D, K_C, Z),$$

где $p(V)$ - вероятность использования уязвимости, $p(T)$ - вероятность реализации угрозы через заданную уязвимость, D - величина значения ущерба от реализации данной угрозы, K_C - уровень контроля информационных ресурсов, Z – затраты.

Необходимо отметить, что вычислять вышеуказанные вероятности крайне сложно. По этой причине предлагается использовать методы нечеткой логики для вычисления риска.

Примерный алгоритм оценивания риска, основанный на положениях нечеткой логики и теории нечетких множеств, учитывающий неопределенности, возникающие в любой корпоративной информационной системе, предлагается реализовать с помощью пакета Fuzzy Logic Toolbox системы MATLAB [9]. С помощью продукционных правил нечеткой логики воспроизводится механизм вывода с учетом пяти входных переменных. Такими переменными, как уже указывалось выше, являются:

- ценность актива,
- уровень угрозы,
- уровень воздействия,
- уровень контроля,
- уровень затрат на восстановление.

Каждая из перечисленных входных переменных оценивается по своей шкале. Например, входная переменная – ценность активов, получается путем экспертных оценок; уровень угроз, предварительно отобранных из БД угроз [6-7] и отфильтрованных с помощью деревьев атак; уровень воздействия (ущерб), полученный путем экспертных оценок. Далее эти входные переменные передаются в Fuzzy Logic Toolbox и выдается значение выходной переменной – риска.

В качестве примера рассмотрим расчет риска в Fuzzy Logic Toolbox с пятью упомянутыми входными переменными: ценность активов - x_A, оценка воздействия (ущерб) – x_D, вероятность реализации угрозы – x_P, опосредовано связанная с уровнем опасности уязвимости (см. Таблицу 3), уровень контроля - x_C, уровень затрат на восстановление – x_Z. Выходная переменная риск – y_R. Применяем модель Мамдани, при этом полагаем, что функции принадлежности первых трех переменных имеют вид гауссовых кривых, а функции принадлежности последних двух имеют трапециевидный вид. Функция принадлежности риска имеет также вид гауссовой кривой. Для лингвистической оценки входных переменных используются диапазоны изменения термов, заданные в Таблицах 1-5 соответственно. Для выходной переменной y_R используем четыре терма с диапазоном значений, приведенными в Таблице 6.

Таблица 6. Выходная переменная Риск (y_R)

№ п/п	Уровень риска	Границы терма «Риск»
1	Незначительный	0 – 0,21
2	Допустимый	0,16 – 0,41
3	Высокий	0,35 – 0,65
4	Критический	0,60 – 1,0

Далее с использованием нечеткой базы знаний вводятся продукционные правила, частично представленные Таблице 7. В предлагаемом примере, в целях его упрощения, дано неполное описание продукционных правил. Для подобной системы из 5-ти входных переменных соответственно с 5-ю, 3-я, 4-я, 4-я и 4-я термами таких правил может быть более 700, а в предлагаемом примере используется только 240.

Таблица 7. Нечеткая база знаний, продукционные правила

	Ценность актива	Уровень угрозы	Уровень воздействия	Уровень контроля	Уровень затрат	Риск
1	Пренебрежимо малая	низкий	незначительный	полный	средний	Незначительный
2	Пренебрежимо малая	низкий	незначительный	высокий	низкий	Незначительный
…						
50	Низкая	низкий	незначительный	высокий	средний	Незначительный
…						
104	Средняя	средний	незначительный	низкий	средний	Допустимый

	Ценность актива	Уровень угрозы	Уровень воздействия	Уровень контроля	Уровень затрат	Риск
…						
164	Высокая	средний	средний	низкий	средний	Высокий
…						
223	Критически высокая	средний	серьезный	средний	средний	Высокий
…						
228	Критически высокая	высокий	серьезный	низкий	средний	Критический
229	Критически высокая	низкий	критический	полный	значительный	Допустимый
…						
240	Критически высокая	высокий	критический	низкий	средний	Критический

После ввода продукционных правил в пакете Fuzzy Logic Toolbox системы MATLAB можно получить нечеткий вывод с конкретными значениями риска. После дефазификации для конкретных значений входных переменных можно получить конкретное значение выходного параметра риска и сравнить его с допустимым значением.

Представленный пакет позволяет осуществить визуализацию зависимости риска от входных параметров (2), то есть представить риск как функцию от переменных (*ценность актива, уровень угрозы, уровень потенциального ущерба, уровень контроля информационных ресурсов. уровень затрат*).

$$(3) \qquad y_R = R\,(x_A, x_P, x_D, x_C, x_Z).$$

При пяти входных параметрах возможно построение десяти трехмерных графиков. При этом на каждом из них можно увидеть зависимость риска от двух параметров при фиксированных значениях трех остальных. Для определения оптимальных значений параметров при допустимом значении риска требуется провести определенную работу, варьируя значениями входных параметров. Естественно, это возможно только в пределах ограничений, наложенных на эти значения, которые имеются при реализации реальных проектов.

В данной работе представлена только часть возможных трехмерных графиков визуализации зависимости риска от значений входных параметров.

Наибольший интерес для целей данной работы представляют зависимости риска от уровня контроля информационных ресурсов и уровня затрат на создание и эксплуатацию системы (Рис. 1). Эти параметры в первую очередь характеризуют степень использования облачных технологий.

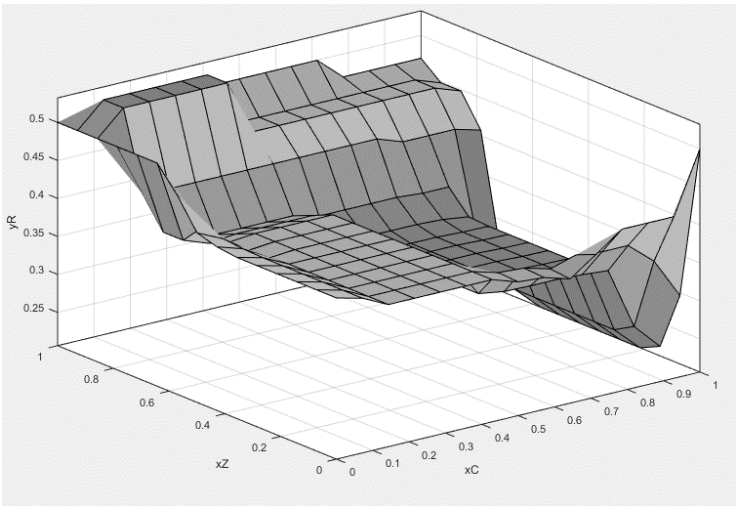

Рис.1 Визуализация зависимости риска от уровня контроля информационных ресурсов x_C и уровня затрат x_Z.

Также представляют интерес зависимости риска от уровня контроля информационных ресурсов и уровня потенциального ущерба (Рис. 2), от уровня контроля информационных ресурсов и уровня активов (объемов и ценности информации в информационной системе) (Рис. 3).

Примеры визуализации приведены при средних значениях других входных параметров, не отображаемых на графиках.

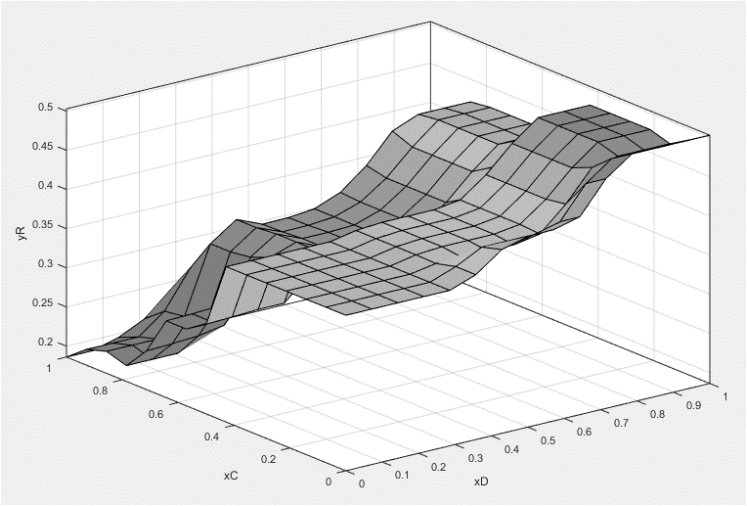

Рис.2 Визуализация зависимости риска от уровня контроля информационных ресурсов x_C и уровня потенциального ущерба x_D.

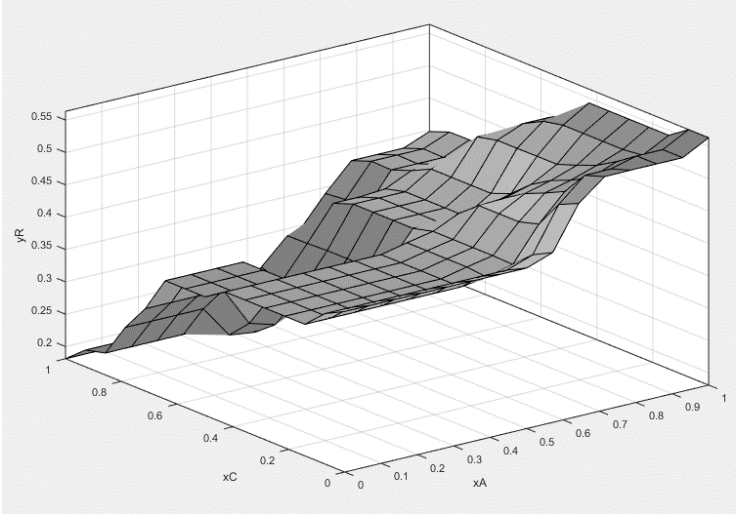

Рис.3 Визуализация зависимости риска от уровня контроля информационных ресурсов x_C и уровня активов x_A.

Зная зависимость риска от значений входных параметров таких, как вероятность реализации угрозы, стоимость активов (ценность информационных ресурсов), потенциальный ущерб, планируемые затраты на создание и эксплуатацию системы, пользуясь предложенной методикой можно определить предельно допустимые варианты использования облачных технологий или предельный объем и структуру данных при использовании конкретных технологий.

Заключение

Предлагаемая методика учитывает уровни угроз, опасности имеющихся уязвимостей, возможный ущерб от реализации угроз, уровень затрат на создание и эксплуатацию системы, а также факторы риска, возникающие при использовании облачных структур, связанные с частичной утратой контроля за собственными информационными ресурсами. Используя данную методику, в условиях большой неопределенности на различных стадиях жизненного цикла корпоративных информационных систем становится возможным:

1. Оценивать уровень риска, как в настоящий момент, так и при последующем накоплении данных.

2. Принимать решение о возможности использования конкретных моделей развертывания корпоративных информационных систем с учетом допустимых пределов использования облачных технологий, предоставляемых сторонними провайдерами.

3. Принимать решения по использованию услуг сторонних провайдеров для создания и эксплуатации корпоративных информационных систем, как отдельных их элементов, так и систем в целом.

4. Определить предельные объемы данных, хранимых в информационной системе, без большого потенциального ущерба.

5. Оптимизировать расходы на создание и эксплуатацию корпоративных информационных систем.

Литература

1. В 2019 году утекло вдвое больше персональных данных, чем годом ранее.- InfoWatch, URL: https://www.infowatch.ru/analytics/digest/19322
2. *Kozlov A., Noga N.* Risk Management for Information Security of Corporate Information Systems Using Cloud Technology / Proceedings of the 11th International Conference "Management of Large-Scale System Development" (MLSD). M.: IEEE, 2018. P. 1-5, https://ieeexplore.ieee.org/document/8551947
3. *Царегородцев А.В., Зеленина А.Н., Савельев В.А*. Двухэтапная процедура количественной оценки риска информационной безопасности облачных вычислений// Моделирование, оптимизация и информационные технологии. – 2017. - №4(19). http://moit.vivt.ru
4. The CORAS Method [Электронный ресурс]. – Режим доступа: www.coras.sourceforge.net/index.html - (Дата обращения: 05.09.2019).
5. *Разумников С.В.* Анализ возможности применения методов OCTAVE, RiskWatch, CRAMM для оценки рисков ИТ для облачных сервисов // Современные проблемы науки и образования, 2014. - № 1. - С. 247-248.
6. Банк данных угроз информационной безопасности. Список уязвимостей. URL: http://www.bdu.fstec.ru/vul
7. Банк данных угроз информационной безопасности. Список угроз. URL: http://www.bdu.fstec.ru/threat
8. *Козлов А.Д., Нога Н.Л.* Риски информационной безопасности корпоративных информационных систем при использовании облачных технологий // Управление риском, 2019. - №3. – С. 31-46
9. Matlab версия 9.6.0 R2019a [Электронный ресурс]. – Режим доступа: https://1progs.ru/matlab/ - (Дата обращения: 05.09.2019)
10. Калькулятор CVSS, версия 3. URL: http://www.bdu.fstec.ru/calc, - 2017