DOI 10.36622/1682-7813.2025.28.2.013
УДК 004.056

РИСКИ РЕАЛИЗАЦИИ КИБЕРАТАК: УПРАВЛЕНИЕ ЗАЩИЩЕННОСТЬЮ СИСТЕМ

Г.А. Остапенко, А.А. Остапенко, Н.С. Харламов, В.А. Швецов, Д.А. Катюрин

Статья посвящена разработке инструментария регулирования рисков на основе гипергеометрического распределения, позволяющего учитывать дискретный характер наступления событий в системах с ограниченным числом критичных элементов. В ходе исследования была систематизирована информация о существующих методах управления рисками, проанализирована информация о дискретных распределениях, на основе которой будет осуществлен выбор наиболее подходящего для рассматриваемой задачи. На основе одного из распределений разработаны методика и алгоритм регулирования рисков, позволяющие получать нужный их уровень в заданном диапазоне ущерба. Результаты исследования представляют собой вклад в области обеспечения информационной безопасности (ИБ) предприятий и могут служить основой для прогнозирования дальнейших рисков на основе имеющейся модели и ситуации.

Ключевые слова: управление рисками, дискретные распределения, гипергеометрическое распределение.

Введение

В условиях роста числа и сложности кибератак становится всё более актуальной задача обеспечения безопасности информационных систем. Традиционные методы оценки риска часто опираются на статистические или обобщенные метрики, не учитывая в полной степени возможность динамического их регулирования рисков. В связи с этим особую значимость приобретает применение математических моделей, основанных на дискретных распределениях вероятностей, которые позволяют более точно описывать и прогнозировать результаты атакующих воздействий и эффективность защитных мер.

Современные подходы к управлению рисками ИБ требуют не только оценки, но и активного регулирования рисков с учетом динамики изменения параметров угроз и ресурсов системы. Разработка методов и алгоритмов, позволяющих адаптивно изменять параметры модели с целью удержания риска в допустимых пределах, представляет собой перспективное направление научных исследований и практического применения [1-3].

Целью исследования является повышение защищенности систем и сетей за счет создания инструментов регулирования рисков на основе дискретных распределений [4].

Исследование аналогов [5-7] позволяет глубже понять эволюцию подходов к управлению рисками ИБ, выявить методологические пробелы и определить перспективные направления для исследований и практического внедрения. Помимо этого, проведенный анализ позволяет выявить следующие ***противоречия*** между:

– универсальной структурой процесса управления рисками и разнообразием практических сценариев реализации кибератак;

– спецификой практических ситуаций, определяющих форму распределения риска, и необходимостью универсального выбора вероятностной модели для формализации угроз;

– стохастической природой риска, зависящей от параметров дискретного распределения, и необходимостью удерживать его на нужном уровне для обеспечения безопасности системы;

Для достижения поставленной цели необходимо решить следующие ***задачи***:

– на основе анализа интернет-источников систематизировать информацию о существующих подходах и методах управления рисками реализации кибератак;

– разработать методику обоснованного выбора дискретных распределений для оценки и управления рисками ИБ, в

зависимости от проектных условий и случайных процессов;

– предложить алгоритм регулирования рисков в нужных диапазонах ущерба для выбранного дискретного распределения.

Процесс управления рисков ИБ

Управление рисками информационной безопасности – итеративный процесс, требующий постоянного контроля над непрерывно-меняющейся ситуацией. В зависимости от сферы деятельности, имеющихся активов и целей менеджмента рисков могут использоваться различные подходы по оценке и регулированию информационной безопасности [1-3].

Суть основных этапов менеджмента рисков остается неизменной, но в рамках постановки задач они могут корректироваться и уточняться. Так, эти этапы могут быть конкретизированы следующим образом:

– выбор анализируемых объектов: на данном этапе необходимо определить область применения процесса управления рисками, ввести организационные и технические ограничения;

– выбор методик оценки рисков: подразумевает определение качественных и количественных методик, которые будут использоваться при оценке риска, шкал, математических принципов, используемых для оценки вероятности;

– идентификация активов: данный этап включает в себя разработку перечня имеющихся активов, определение их ценности для компании, выделения из них тех, которые представляют особую важность для организации;

– анализ угроз и их последствий, выявление уязвимых мест в защите. Данный этап ориентирован на обработку исходных данных, поскольку весь процесс управления рисками в самом начале разработки информационной системы опирается на построение модели угроз. Она является отправной точкой для изучения возможных рисков организации ввиду того, что модель угроз позволяет расписать сам риск, который складывается из угрозы, уязвимости и актива. Это позволяет понять какая угроза будет реализована, через какую уязвимость и на какой актив направлена;

– оценка рисков: является одним из центральных элементов процесса управления рисками ввиду того, что своевременное определение, обработка рисков позволяет своевременно снизить вероятность возникновения ущерба как репутационного, так и материального. На данном этапе все выявленные риски анализируются, определяется их потенциальное влияние, что является отправной точкой для принятия решений о дальнейших действиях по его регулированию или о выборе мер и необходимых средств защиты информации;

– обеспечение безопасности, должно основываться на своевременном применении всего комплекса мер в соответствии с нормативно-правовыми актами и мнением специалистов, однако их необходимо соразмерять с возможностями самой организации и информационной системы;

– реализация и проверка выбранных мер: данный процесс включает в себя непосредственное внедрение в эксплуатацию выбранных средств защиты информации и наладка их работы, их тестирование и испытанием системы в совокупности с реализованными мерами. По окончанию этих мероприятий осуществляется оценка соответствия систем защиты информации требованиям регуляторов в области информационной безопасности;

– оценка остаточного риска является ключевым этапом управления рисками, при котором определяется уровень риска, остающийся после внедрения всех запланированных мер защиты. Другими словами, мы имеем ситуацию, при которой уровень текущего риска может быть ниже уровня остаточного риска. В таком случае предпринимать дополнительные меры по снижению информационных рисков для указанного объекта сети не нужно. Это подчеркивает также тот факт, что полное устранение всех рисков просто не представляется возможным или практичным. При этом проблема современных подходов к оценке риска заключается в том, что большинство из них не рассматривают разделение механизмов защиты на типы, которое позволило бы более качественно проанализировать существующую систему защиты на предприятии.

Использование дискретных распределений

Риск – произведение величины ущерба на вероятность её наступления. Данная функция является стохастической, поскольку его

составляющие, такие как нанесенный атакой ущерб, вероятность успешности реализации атаки, набор реализованных угроз, являются неопределенными и случайными параметрами. В связи с этим свойством риска целесообразно использовать вероятностные инструменты – дискретные распределения, такие как биноминальное распределение, мультиномиальное распределение, гипергеометрическое распределение, геометрическое распределение, распределение Пуассона, распределение Паскаля [4].

Дискретные распределения позволяют формально описать случайные события, которые происходят с определенной вероятностью. Их целесообразно использовать ввиду не детерминированности современных кибератак, поскольку они зависят от большого количества факторов и могут иметь разные последствия. Благодаря данным распределениям можно описывать последствия как единичных, так и множественных атак.

Выбор распределения будет зависеть от следующих факторов:

– типа процесса, подразумевающего один процесс или несколько категорий исходов;

– характера событий – независимые/зависимые, с постоянной/меняющейся вероятностью;

– дисперсионных характеристик – равенство или неравенство среднего и дисперсии. В данной ситуации сравнение дисперсии и математического ожидания позволит определить характер случайного процесса, тип стохастической зависимости между событиями, адекватность модели для описания данных.

Выбор распределения должен отражать не только статистические свойства данных, но и природу моделируемых угроз. В ИБ нет идеальных моделей, но правильный выбор распределения сокращает «слепые зоны в оценке рисков». Графически выбор дискретного распределения представлен на рис. 1.

Алгоритм регулирования риска с использованием гипергеометрического распределения

Гипергеометрическое распределение удобно использовать для анализа рисков и последствий, связанных с ограниченными выборками без возвращения, то есть в ситуациях, когда имеется фиксированный набор объектов и выбираются подмножества без «возвращения» или повторного использования. При этом гипергеометрическое распределение опирается на фиксированные, дискретные величины.

Данное распределение позволяет рассчитать вероятность, что при m совершенных атаках, ровно x из них задействуют критичные уязвимости. То есть уязвимости, через которые потенциальная атака может быть успешно реализована. Распределение имеет следующий вид (1) [8-9]:

$$p(x;n,k,m)=\frac{C_k^x C_{n-k}^{m-x}}{C_n^m};$$
$$x \le k; m-x \le n-k; \qquad (1)$$

где x – число успешных атак на критичные уязвимости;

m – число совершенных атак, задействующих некоторую уязвимость;

k – число критичных уязвимостей;

n – общее число уязвимостей.

Данное распределение может быть использовано при изучении «слепой атаки» – сценария, при котором злоумышленник не располагает информацией о конфигурации системы и возможных точках компрометации, и потому осуществляет атаки на случайно выбранные уязвимости, рассчитывая на попадание в критичные. Подобная атака может моделироваться с помощью гипергеометрического распределения, поскольку выборка осуществляется без возвращения и без априорного знания о наличии «критичных уязвимостей». Схема реализации «слепой атаки» представлена на рис. 2.

Анализируя ограничения гипергеометрического распределения, можно отметить, почему они могут выполняться в рамках обеспечения информационной безопасности:

$x <= k$ – данное условие означает, что нельзя реализовывать в атаке больше критичных уязвимостей, чем было совершено атак;

$m - x <= n - k$ – данное условие означает, что число атак на некритические уязвимости $(m - x)$ не превышает их доступное количество $n - k$.

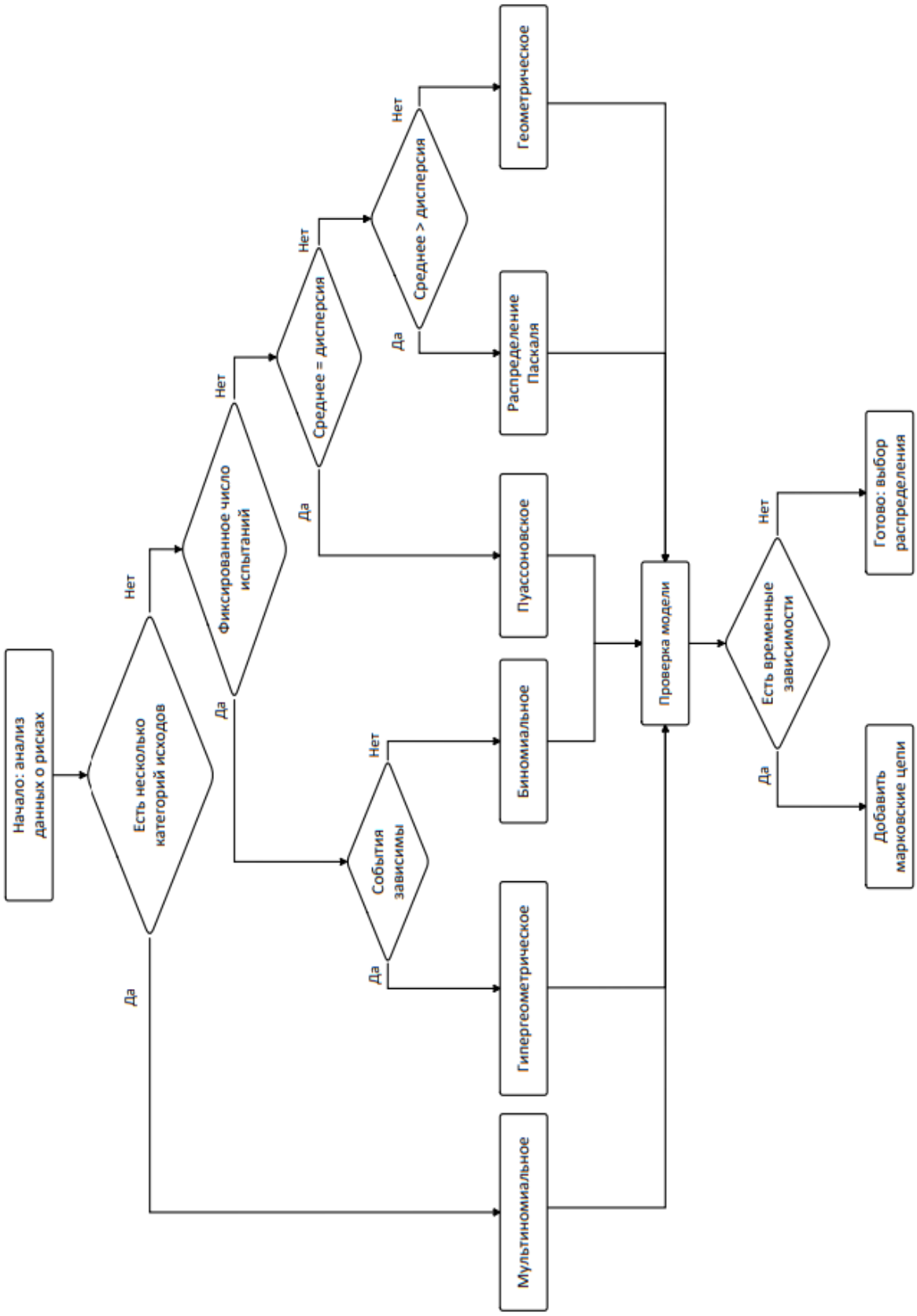

Рис.1. Выбор дискретного распределения

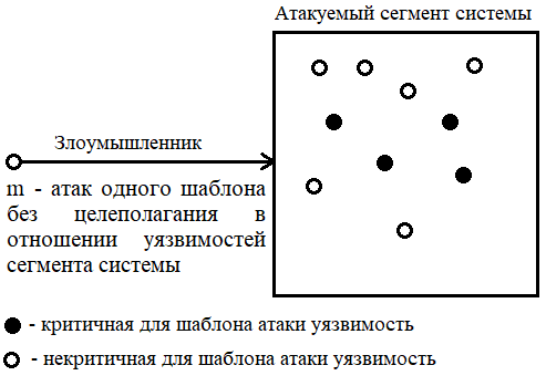

Рис. 2. Схема реализации «слепой атаки»

Закрыть все уязвимости проблематично, поскольку это требует:

– времени на анализ и тестирование;

– качественных специалистов, которые являются наиболее редким ресурсом ввиду мирового их дефицита, превышающего 3 миллиона человек. Спрос на таких специалистов растет с большим темпом, по сравнению с интенсивностью появления новых кадров;

– финансов на обновление, новые средства защиты информации.

Даже если известно, что на текущий момент «закрыты» все уязвимости на следующий день может выйти обновленная версия программного обеспечения с новыми критичными уязвимостями, или же злоумышленники могут найти новые в той же версии.

Само количество атак m должно быть меньше количества критичных уязвимостей k, поскольку если m>k, то часть атак не может попасть в критичные уязвимости ввиду недостаточности целей. Более того, вероятность «успешных» атак при большом m будет искажена и переоценена.

Критичные уязвимости – объекты, через которые может быть реализована атака. Если последних больше, чем уязвимостей вообще, то имеем ситуацию, когда атаки «бьют» в пустоту (в реализованные уязвимости) или не учитывается ограниченность возможностей атакующих, что маловероятно в условиях защищенной ИС.

Анализируя указанные параметры, можно сделать вывод, что специалист по ИБ может повлиять только на параметр k, поскольку: x – стохастическая величина, характеризующаяся числом успешных атак, n – общее число уязвимостей, определяемое исходным состоянием системы (обычно зафиксировано технической архитектурой ПО), m – количество атак, определяемое действиями противника и используемыми уязвимостями. Возвращаясь к k, ИБ-специалист может управлять количеством критичных уязвимостей, устраняя уязвимость, снижая её доступность, но саму критичность уязвимости корректировать не может, поскольку это является внешне заданным статистическим параметром, определяемым калькуляторами CVSS, OWASP, EPSS, а не тем, что может напрямую изменить специалист по ИБ. Поэтому единственным способом корректировки этого параметра является не уменьшение критичности какой-то конкретной уязвимости, входящей в это множество, а деятельность через её окружение и контекст эксплуатации. Такая деятельность может подразумевать ограничение сетевого доступа, удаление программного компонента, отключение сервисов и служб, сегментация. Иными словами, уязвимость по-прежнему критична, но исключена из атакуемого множества, и потому не входит в n.

Помимо этого, целесообразно использовать дополнительные механизмы, делающие уязвимость непригодной для эксплуатации или рассматривать только те уязвимости, которые могут быть эксплуатируемы в текущей архитектуре.

С точки зрения извлечения без возвращения гипергеометрическое распределение должно быть учтено при исключении уязвимостей:

– проэксплуатируемых, чтобы не предоставить злоумышленнику повторную возможность успешной атаки;

– некритичных, но уже выявленных, для которых злоумышленник может найти подходящий шаблон атаки.

Однако в рамках регулирования возникает необходимость учитывать ограничения ресурсов, затрачиваемых на управление числом критичных уязвимостей. С этой целью введем понятия энергии управления как агрегированной меры на реализацию управляющих воздействий.

Энергия управления (E) – мера затрат или усилий, необходимых для того, чтобы изменить состояние системы и привести её к цели. В данном случае необходимо привести исходную систему к состоянию, при котором

уровень риска в заданном диапазоне не превышает допустимого значения. То есть энергией управления является метафора затрачиваемых ресурсов, что делает задачу более реалистичной.

Необходимо также помнить, что управляющее воздействие в модели регулирования риска – любое целенаправленное действие, снижающее риски наступления ущерба за счет уменьшения k_t. Поэтому на него целесообразно вводить ограничение, связанное с доступной энергией управления (бюджет, часы экспертов). Ограничение позволит не перезагружать частыми действиями систему, сохранять ресурсы. Его можно представить в виде формулы (2):

$$\sum_{t=0}^{T} |u_t| \leq E_{max}. \qquad (2)$$

При построении системы защиты используется формальная экстраполяция, то есть прогнозирование угроз и рисков на основе формализованных моделей и текущих данных, с целью предварительного построения или корректировки системы защиты еще до наступления событий. Это позволит наблюдать динамику в будущем, основываясь на предположении, что текущие тенденции будут продолжаться. При процессе моделирования введем прирост числа критичных уязвимостей λ_t (появление новых критичных уязвимостей) и снижение их числа μ_t – величины, которые будут неизменными в процессе последующей эксплуатации защищенной информационной системы.

Параметр λ_t можно рассчитать следующим образом (3):

$$\lambda_t \approx \Delta k_t^+. \qquad (3)$$

Получаем положительный прирост количества уязвимостей Δk_t^+ за шаг t.

Параметр μ_t можно рассчитать следующим образом (4):

$$\mu_t \approx \Delta k_t^-. \qquad (4)$$

Получаем количество устраненных уязвимостей Δk_t^- за шаг t без учета управляющего воздействия u_t.

Сами переменные лежат в следующих диапазонах:

$\lambda_t \in [0, n - k_t]$, при этом максимум достигается, если все имеющиеся оставшиеся уязвимости из общего числа становятся критичными на текущем шаге;

$\mu_t \in [0, k_t]$, максимум достигается, если все текущие критичные уязвимости устраняются без участия управления.

Относительно разного поведения переменных может реализовываться регулирование риска, смещая график и соответственно значения риска в меньшую сторону или большую. С учетом этих параметров и управляющего воздействия u_t получаем следующее выражение (5):

$$k_{t+1} = k_t + \lambda_t * u_t - \mu_t * u_t. \qquad (5)$$

Значение управляющего воздействия лежит в диапазоне от 0 до 1:

$u_t = 0$ – нет управления, система развивается «естественным образом» (появление уязвимостей не подавляется, устранение не ускоряется);

$u_t = 1$ – максимальное управление (ресурсы максимально брошены на контроль и устранение.

Если необходимо уменьшать значение k_t для увеличения уровня риска при меньших значениях ущерба, необходимо, чтобы число критичных уязвимостей снижалось, что может осуществляться за счет следующих действий:

u_t – активно управляем за счет контроля критичных уязвимостей, внедрения патчей;

λ_t – прирост числа критичных уязвимостей нужно стараться держать низким за счет превентивных мер, предиктивного анализа;

μ_t – рост данного параметра помогает снижению k_t.

Таким образом имеем два контролируемых параметра u_t и μ_t, которые и вносят основной вклад в снижение риска, компенсируя λ_t.

Имеем и обратную ситуацию – контролируемо увеличить k_t, чтобы перераспределить риск и сделать его менее концентрированным. В таком случае имеем следующее поведение переменных:

k_t – необходимо целенаправленно увеличивать, не запуская ситуацию (держа все под

контролем), для получения нового значения на следующем шаге;

u_t – целенаправленно временно ослабляем управляющее воздействие;

λ_t – прирост числа критичных уязвимостей обусловливается внедрением нового кода, расширением зон сканирования;

μ_t – параметр стабилен, мал, при этом не мешает росту k_t.

Чтобы избежать перерасход энергии необходимо контролировать ожидаемый остаток энергии на каждом шаге. Тогда получаемый остаток выходит из следующей формулы (6):

$$E_{\text{ост}} = E_{max} - \sum_{t=0}^{T} |u_t| . \qquad (6)$$

При этом целесообразнее связать управляющее воздействие u_t с параметрами положительного и отрицательного прироста количества критичных уязвимостей и ввести соответствующие коэффициенты $\alpha, \beta \in [0,1]$ — коэффициенты чувствительности управления к интенсивностям. Эти коэффициенты определяются априорно для разных классов систем и меняются редко и сложно. Получаем, что, регулируя λ_t, μ_t, u_t, можем регулировать итоговую переменную k_{t+1}.

Тогда получаем следующую формулу расчета k_{t+1} (7):

$$k_{t+1} = k_t + \lfloor \lambda_t * (1 - \alpha u_t) \rfloor - \\ - \lfloor \mu_t * (1 + \beta u_t) \rfloor ; \qquad (7)$$

где $\lambda_t * (1 - \alpha u_t)$ – чем больше управление, тем меньше темп появления уязвимостей;

$\mu_t * (1 + \beta u_t)$ – чем больше управление, тем больше темп устранения уязвимостей.

При этом, если $\alpha = 0$, то при даже при максимальном управлении 1 никакого влияния на появление уязвимостей нет, если же $\alpha = 1$, то при $u_t = 1$ прирост уязвимостей может быть полностью подавлен. Управление способствует понижению интенсивности появления уязвимостей.

В случае с β, если $\beta = 0$, управление не ускоряет устранение, если $\beta = 1$, при $u_t = 1$ снижение (отрицательный прирост) удваивается. Управление увеличивает скорость устранения уязвимостей.

Если в рамках работы над биномиальным распределением целесообразно было рассматривать отдельные уязвимости в качестве объектов, то в случае гипергеометрического распределения можно рассматривать систему, содержащую уязвимости или несколько сегментов системы, так же содержащие уязвимости.

Эти сегменты можно считать независимыми друг от друга, поскольку каждый сегмент может обслуживать разные процессы, сервисы и отделы, иметь свой набор уязвимостей. Если атака на один сегмент не влияет напрямую на другой, то события (согласно теории вероятностей) можно считать независимыми. Внутренние политики также могу делать сегменты условно-изолированными. Поэтому, целесообразно агрегировать риск по нескольким объектам или сегментам. Однако, если появятся взаимосвязи между сегментами (атака на один сегмент открывает возможность для атаки на другой), то целесообразно переходить к совместным распределениям или моделям с зависимостями, поскольку простое сложение не будет отражать реальную картину.

Считая x величиной нормированного ущерба, можно оценить риск по формуле (8):

$$Risk = x \frac{C_k^x C_{n-k}^{m-x}}{C_n^m}, \qquad (8)$$

где $x = 1(1)10$.

Однако в этом случае мы можем иметь большой разброс значений рисков как на рис. 3.

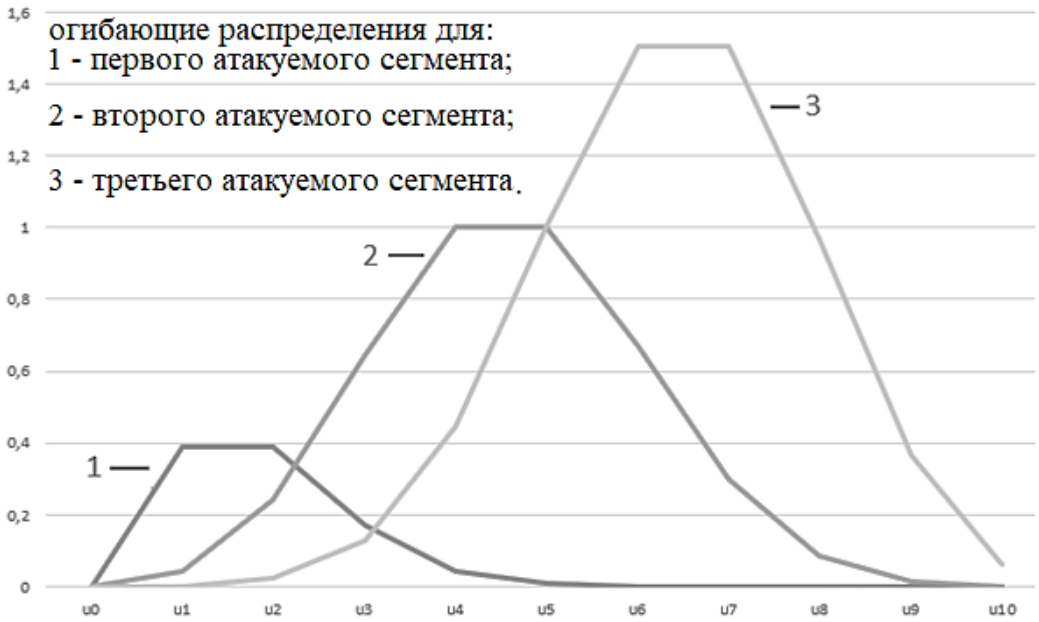

Рис. 3. Огибающие распределений с учетом ущерба x

Считая x ущербом, вводим дополнительно величину α_i, отвечающую за долю потерь защищаемого i-го сегмента. Этот параметр может служить локальным инструментом чувствительности, учитывающим специфику конкретного сегмента, что также позволяет решить вопрос с перекосом в системе обеспечения безопасности (рис. 3).

Отсюда ущерб будет равен $x*\alpha_i$. При перераспределении доли потерь можно оценить влияние каждого сегмента на суммарный риск.

При перераспределении огибающие примут вид, как это показано на рис. 4.

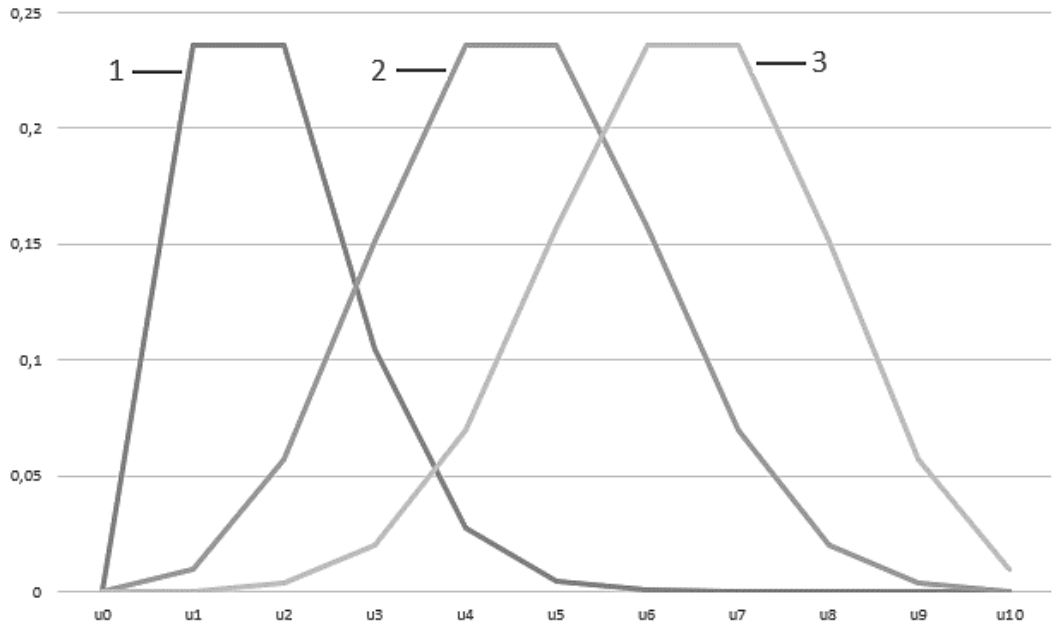

Рис. 4. Огибающие распределений с учетом ущерба $x*\alpha_i$

Работая с суммарным риском, вводим дополнительно C_j – ценность ресурса, при реализации x_j – числа реализованных атак (j = 0(1)m_i), перераспределяя который огибающие примут необходимый вид.

Тогда суммарный риск рассчитывается по формуле (9):

$$Risk_{total} = \sum_{j=1}^{m} (Cj \sum_{i=1}^{L} Risk_{ij}), \qquad (9)$$

где L – количество объектов (сегментов сети).

Графически итоговый результат представлен на рис. 5.

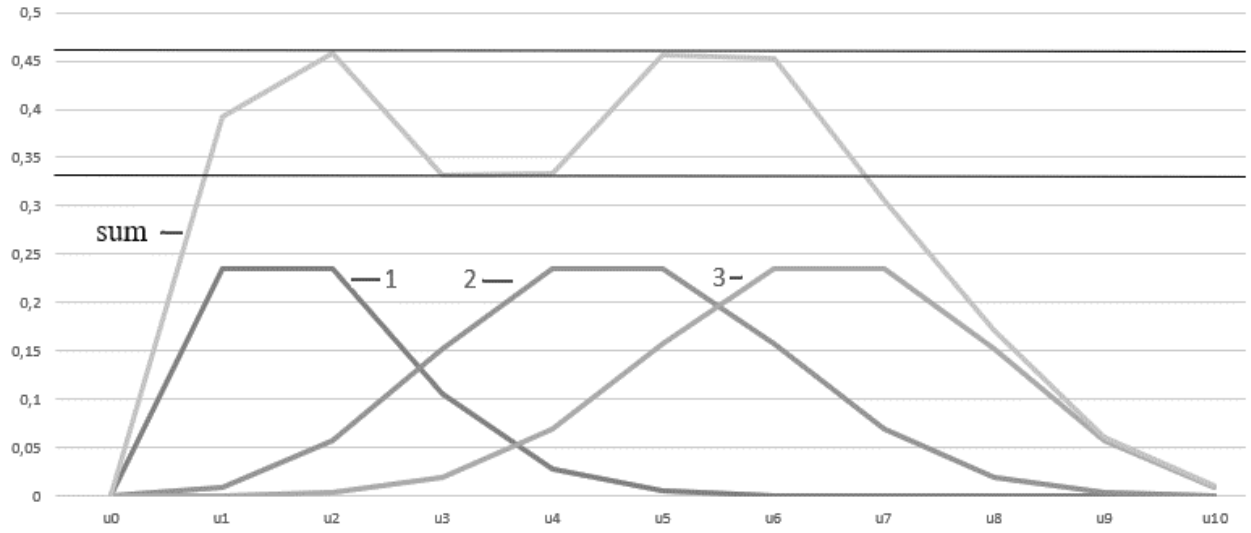

Рис. 5. Огибающие распределений (отдельных огибающих и суммарный)

Однако при таком расчете получаем, что сумма вероятностей превышает 1, что не может быть, поэтому чтобы сохранить интерпретацию результата как вероятностного распределения, его необходимо нормировать. Поэтому получаем следующую формулу (10):

$$Risk_{total}^{norm} = \frac{1}{L} \sum_{z=1}^{L} Risk_z . \qquad (10)$$

Нормировка позволит корректно сравнить риски разных событий и сделать осмысленные выводы. Более того, если вероятности не нормированы, ожидаемый риск может быть завышен или занижен из-за некорректных весовых коэффициентов. Многие математические методы предполагают работу с нормированными распределениями. Ненормированные данные могут привести к численной неустойчивости или ошибкам в дальнейших расчетах.

Регулирование осуществляется за счет перераспределения C_j и корректировки параметров самого распределения. Имея исходную агрегированную огибающую, возвращаемся к её составляющим, меняем параметры распределений, агрегируем их и перераспределяем Ci для поддержания риска в заданном диапазоне.

В итоге получаем алгоритм с использованием принципа обратной связи, основанный на динамическом обновлении параметра k_t на каждом шаге времени t с учётом текущего состояния системы (k_t), положительного и отрицательного прироста (λ_t, μ_t), управляющих воздействий (u_t), которые как раз и корректируют эти величины. Данный принцип позволяет регулировать и динамически балансировать систему в реальном времени через u_t.

Предложенный подход ближе к реальным условиям функционирования информационных систем, где уязвимости могут устраняться, а меры защиты адаптироваться к изменяющимся угрозам.

Таким образом, сам алгоритм регулирования рисков с использованием гипергеометрического распределения можно представить следующим образом (рис. 6).

Заключение

Проведенное исследование позволяет сформулировать полученные ***результаты***:

– систематизированная информация о существующих подходах и методах управления рисками реализации кибератак;

– методика обоснованного выбора дискретных распределений для оценки и управления рисками ИБ, в зависимости от проектных условий и случайных процессов;

– разработан алгоритм регулирования рисков в нужных диапазонах ущерба для выбранного дискретного распределения.

Алгоритм позволяет обеспечить пошаговое регулирование, выстроить цепочку управляющих воздействий, определить сколько усилий нужно потратить, чтобы удержать систему в безопасной зоне и при ограниченности ресурсов минимизировать E, не выходя за допустимые значения ущерба**.**

Помимо регулирования уровня риска данный алгоритм можно применить для управления защищенности, понимаемой, как состояние объекта или системы, при котором риск наступления ущерба остается в допустимых границах. Управление защищенностью в рамках рассматриваемого алгоритма означает – поддержание количества уязвимых элементов k_t, перераспределение риска в сторону меньших ущербов.

Алгоритм позволит динамически моделировать и корректировать состояние защищенности через соответствующий ряд параметров.

Список литературы

1. Управление рисками информационной безопасности // URL: https://www.securityvision.ru/blog/upravlenie-riskami-informatsionnoy-bezopasnosti-konspekt-lektsii/ (Дата обращения: 09.05.2025).

2. Математическое моделирование рисков: шаманство или кибернетика? // URL: https://www.securityvision.ru/blog/matematicheskoe-modelirovanie-riskov-shamanstvo-ili-kibernetika/. (Дата обращения: 09.05.2025).

3. Вишняков Я.Д. Общая теория рисков_Вишняков / Я.Д. Вишняков, Н.Н. Радаев. // URL: https://academia-moscow.ru/ftp_share/_books/fragments/fragment_21013.pdf. (Дата обращения: 09.05.2025).

4. Сигорский В.П. Математический аппарат инженера / В.П. Сигорский – 2-е изд., стереотип. «Техника. – 768 с.

5. Кудрявцев А.А. Введение в количественный риск-менеджмент / А.А. Кудрявцев, А.В. Родионов. – СПб.: Изд-во С.Петерб. ун-та, 2016. – 192 с.

6. Остапенко А.А. Методики и алгоритмы риск-анализа успешности реализации массированных кибератак / А.А. Остапенко // Информация и безопасность. 2024. т. 27. Вып. 3. с. 401-420.

7. Калашников А.О. Модели управления информационными рисками сложных систем / А.О. Калашников, Е.В. Аникина // Информация и безопасность. 2020. Т. 23. Вып. 2. С. 191-202.

8. Калашников А.О. Управление информационными рисками сложной сети на основе метода стохастического имитационного моделирования (часть 1) / А.О. Калашников, Е.В. Аникина // Информация и безопасность. 2019. Т. 22. Вып. 1. С. 6-13.

9. Гипергеометрическое распределение // URL: https://ru.wikipedia.org/wiki. (Дата обращения: 09.05.2025).

10. Егоров А.И. Основы теории управления / А.И. Егоров // М.: ФИЗМАТЛИТ, 2007. – 504 с.

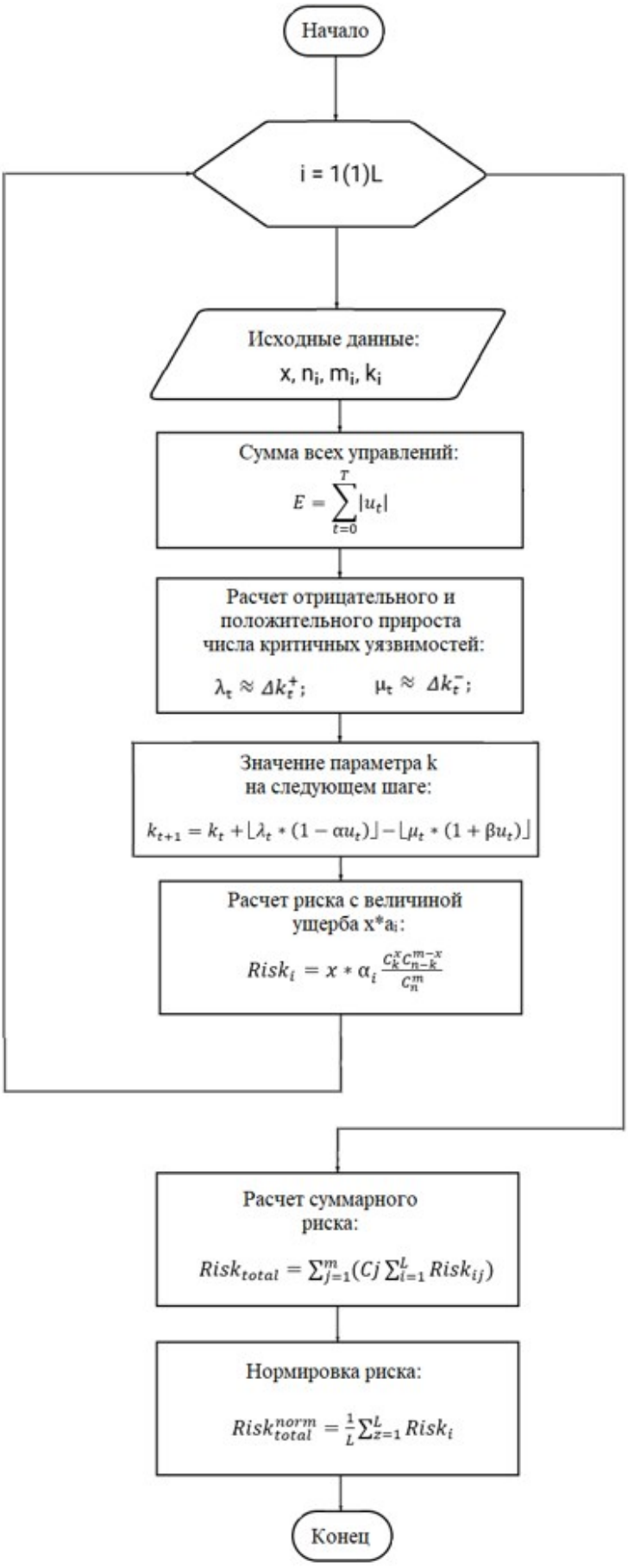

Рис. 6. Алгоритм регулирования риска

Финансовый университет при Правительстве Российской Федерации
Financial University under the Government of the Russian Federation

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 17.05.2025

Информация об авторах

Остапенко Григорий Александрович – д-р техн. наук, проректор Финансового университета при Правительстве Российской Федерации, e-mail: ost@fa.ru

Остапенко Александр Алексеевич – аспирант, Воронежский государственный технический университет, e-mail: alexostap123@gmail.com

Харламов Никита Сергеевич – студент, Воронежский государственный технический университет, e-mail: harlam040@mail.ru

Швецов Владимир Алексеевич – студент, Воронежский государственный технический университет, e-mail: shvecov.vova@lenta.ru

Катюрин Дмитрий Александрович – студент, Воронежский государственный технических университет, e-mail: d.katiurin@yandex.ru

RISKS OF IMPLEMENTING CYBER-ATTACKS: MANAGEMENT SYSTEM SECURITY

G.A. Ostapenko, A.A. Ostapenko, N.S. Kharlamov, V.A. Shvetsov, D.A. Katyurin

The article is devoted to the development of risk management tools based on hypergeometric distribution, allowing to take into account the discrete nature of the occurrence of events in systems with a limited number of critical elements. In the course of the study, information on existing risk management methods was systematized, information on discrete distributions was analyzed, on the basis of which the most suitable one for the task under consideration will be selected. Based on one of the distributions, a methodology and algorithm for risk management were developed, allowing to obtain the required level in a given range of damage. The results of the study represent a contribution to the field of ensuring information security (IS) of enterprises and can serve as a basis for predicting further risks based on the existing model and situation.

Keywords: risk management, discrete distributions, hypergeometric distribution.

Submitted 17.05.2025

Information about the authors

Grigory A. Ostapenko – Dr. Sc. (Technical), Vice-Rector of the Financial University under the Government of the Russian Federation, e-mail: ost@fa.ru

Alexander A. Ostapenko – graduate student, Voronezh State Technical University, e-mail: alexostap123@gmail.com

Nikita S. Kharlamov – student, Voronezh State Technical University, e-mail: harlam040@mail.ru

Vladimir A. Shvetsov – student, Voronezh State Technical University, e-mail: shvecov.vova@lenta.ru

Dmitry A. Katyurin – student, Voronezh State Technical University, e-mail: d.katiurin@yandex.ru