А.Ж. Абденов, В.А. Трушин, Г.А. Абденова, Ю.А. Иноземцева

Методика расчета рисков на основе объективных и субъективных оценок в соответствующих узлах SIEM-системы

Аннотация. В работе рассматриваются вопросы управления рисками в соответствующих узлах SIEM-системы для целей организации в режиме реального времени, рекомендаций защиты информации в информационных системах предприятия. Расчеты рисков основаны на объективных оценках вероятностей реализации неблагоприятных событий, предсказаний величин ущербов от нарушений информационной безопасности. В рекомендации предлагается включить организацию эффективного выбора средств по защите информационных ресурсов при финансовых ограничениях на приобретение этих средств.

Ключевые слова: оценка риска, защита информации, информационные ресурсы, информационная система, неблагоприятные события, объективные оценки, ущербы.

Введение

Разработка систем комплексной, активной, с элементами интеллектуальных сервисов защиты конфиденциальной информации (КИ) требует успешной реализации различных мероприятий по защите информационных ресурсов (ИР) в компьютерных системах (КС). Эти мероприятия предполагают решение целого ряда задач, в частности, создание системы мониторинга угроз безопасности. Системы мониторинга реализуют текущий и апостериорный подходы к защите информации и основной целью своего создания имеют снижение количества неблагоприятных событий (НС) воздействующих на ИР компьютерных систем до минимального уровня риска и минимизацию возникающего при этом ущерба.

Одним из наиболее перспективных и эффективных направлений в создании систем мониторинга угроз безопасности в настоящее время считаются SIEM-системы (SIEM-Security Information and Event Management), обеспечивающие управление информацией и событиями безопасности. Основной целью построения и функционирования SIEM-системы является значительное повышение уровня информационной безопасности (ИБ) в информационной инфраструктуре за счет обеспечения возможности в режиме реального времени манипулировать информацией о безопасности, осуществлять активное управление событиями безопасности [1]. Предполагается, что активное управление инцидентами и событиями безопасности основывается на автоматических механизмах, использующих накопленную информацию о предыстории анализируемых событий и прогнозе будущих событий. А также на автоматической подстройке параметров мониторинга событий к текущему состоянию защищаемой системы и выдаче рекомендаций для корректировки политики информационной безопасности на основе эффективного использования средств защиты ИР в КС [2].

Обсуждение вопросов, возникающих в разрабатываемых SIEM-системах для сервисных информационных инфраструктур, проводится в проекте MASSIF (MAnagement of Security information and event in Service InFrastructure - Управление информацией и событиями безопасности в инфраструктурах услуг) седьмой рамочной программы Европейского Союза [1].

Мы предполагаем, что одним из обсуждаемых вопросов в рамках проекта MASSIF должны быть вопросы наполнения отдельных узлов SIEM-системы возможностями решения задач прогнозирования, фильтрации и оптимизации использования средств защиты ИР в КС [3, 4]. Для достижения данной цели SIEM-система должна обладать возможностью успешного решения следующего комплекса задач:

- сбора, обработки и анализа событий безопасности, поступающих в систему из множества гетерогенных источников;
- обнаружения в режиме реального времени атак, нарушений критериев и политики безопасности;
- анализа и управления рисками в ИС на основе объективных и экспертных оценок [3];
- оперативной оценки защищенности информационных, телекоммуникационных и других критически важных ИР;
- проведения расследований инцидентов;
- принятия эффективных решений по защите информации [4];
- формирования отчетных документов.

Основными исходными данными, которые используются SIEM-системой для решения указанных задач, являются записи различных журналов аудита (logs), протоколирующие события в информационной инфраструктуре, называемые «событиями безопасности». Данные события отражают такие действия пользователей и программ, которые могут оказать влияние на ИБ. Из общего множества событий безопасности SIEM-система должна в режиме реального времени находить такие события безопасности, которые свидетельствуют об атаках или иных воздействиях, причем традиционные методы поиска такой информации достаточно трудоемки.

Разработанные в европейских государствах SIEM-системы имеют архитектуру "агенты–хранилище данных–сервер приложений" [1, 2]. Агенты выполняют сбор событий безопасности, их первоначальную обработку, фильтрацию и классификацию. Собранные, отфильтрованные, классифицированные информации о событиях безопасности поступают в хранилище данных или репозиторий (хранилище данных в SIEM-системах), где они хранятся во внутреннем формате представления с целью последующего использования и анализа сервером приложений. Серверы приложений анализируют информацию, хранимую в репозитории, и преобразуют ее для выработки предупреждений, других рекомендаций в режиме реального времени, а также управленческих решений по защите информации.

В перспективных SIEM-системах (т.е. в системах нового поколения) к числу расширений функциональных наполнений узлов SIEM-системы следует добавить анализ событий, инцидентов и их последствий, принятие решений и визуализацию информации. Раскроем примерное содержание некоторых механизмов по уровням иерархии SIEM-системы:

- нормализация означает приведение форматов записей журналов, собранных из различных источников к единому внутреннему формату, который затем будет использоваться для их хранения и последующей обработки;
- фильтрация событий безопасности заключается в корректировке текущих оценок состояния защищенности ИР в КС и расчеты этих оценок на будущий интервал времени;
- приоритезация определяет значимость и критичность событий безопасности на основании правил, определенных в системе;
- анализ событий, инцидентов и их последствий включает процедуры моделирования событий, атак и их последствий, анализа уязвимостей, оценок риска, прогнозирование и фильтрации оценок НС и инцидентов;
- система поддержки принятия решений (СППР) определяет выработку мер по оптимизации и реконфигурированию средств защиты с целью предотвращения атак на КС;
- генерация отчетов и предупреждений означает формирование, передачу, отображение и (или) печать результатов функционирования.

В статье будут предложены и раскрыты некоторые элементы наполнения отдельных узлов SIEM-системы алгоритмами решения задач расчета риска на основе объективных и экспертных оценок, а также расчета оценок предсказания и фильтрации количества НС, величину ущерба и оптимизации использования средств защиты ИР в КС [3, 4].

1. Оценивание риска в информационных системах на основе объективных и экспертных оценок

Основанный на рисках подход к оценке потенциального ущерба от атак нарушителей и

выбору мер для его минимизации получил название "Управление рисками". Под управлением рисками подразумевается полный комплекс алгоритмов и мероприятий из ряда выполняемых последовательно процессов, что соответствует существующим международным стандартам и практике управления рисками на предприятиях [5]: идентификация, анализ и принятие рисков, мониторинг и пересмотр. В существующих методиках управления рисками их идентификация осуществляется различными методами, такими как командные «мозговые штурмы», анализ архитектуры системы, операционное моделирование, анализ сценариев, исследования HAZOP (HAZard and OPerability studies). HAZOP – это признанный лидер при анализе рисков на особо опасных объектах с катастрофичными последствиями [6]. На современном этапе одна из методик управления рисками основана на экспертных оценках [7].

Основанием расчета и анализа рисков являются статистические данные из репозитория SIEM-системы, собранные в процессе идентификации рисков, а результаты работы системного аналитика используются лицами или процессами из соответствующих узлов SIEM-систем, принимающими решения в СППР [8]. В настоящее время модели анализа и оценки рисков проходят стадию развития [9], которые рассматривают управление рисками как принятие решений в условиях неопределенности, а количественные показатели риска – как критерии принятия альтернативных или взаимодополняющих решений в процессе какой-либо деятельности.

Оценки риска рассчитываются в зависимости от вероятности реализации НС в ИС. Различают объективные и субъективные вероятности наступления НС. Оценка объективных вероятностей наступления НС – одна из важных задач в алгоритме расчета оценок риска. При этом использование этих объективных оценок для повышения эффективности расчетов оценок риска в ИС предприятия является важной задачей в методике расчета оценок потенциального ущерба от атак нарушителей.

1.1. Алгоритм расчета объективной вероятности реализаций НС в КС

В работе [3] предлагалась одна версия методики расчета объективной вероятности реализаций НС в КС. Из списка множества существующих видов НС, имеющихся в репозитории SIEM-системы, выделяется некоторое существенное подмножество видов НС, приводящих к ощутимому нарушению безопасности ИР в КС. Это подмножество обозначим через

$$O = \{O_{i_1}, O_{i_2}, \ldots, O_{i_m}\},$$

где O_{i_1} – количество НС относительно нарушения запуска отдельных узлов КС; O_{i_2} – количество НС относительно неверного набора информации применительно к конкретному информационному процессу и обработке данных и т.д.

После построения подмножества O, переходим к анализу свойств элементов подмножества на основе количественных показателей НС и соответственно величины ущерба, имевшей место в прошлом. Математическое ожидание ущерба, вызываемого i-м НС за время ΔT (например, 1 месяц), можно представить формулой:

$$e(O_i, \Delta T) = M[e(O_i) \cdot f_i], i = \overline{1,m}, \qquad (1)$$

где $e(O_i)$ – случайная величина ущерба уже случившегося НС при единичном наступлении НС; f_i – случайная величина количества НС i-го вида за время ΔT; m – общее количество всех видов уже свершившихся НС.

Если НС не имеют последствия в том смысле, что ущерб от каждого НС независим, то

$$e(O_i, \Delta T) = M[e(O_i)] \cdot M[f_i], \quad i = \overline{1,m}, \qquad (2)$$

а ущерб для всего множества существенных НС будет определяться с помощью соотношения:

$$E(O, \Delta T) = \sum_{i=1}^{m} M[e(O_i)] \cdot M[f_i]. \qquad (3)$$

Алгоритм 1

Шаг 1.1. Для простоты будем рассматривать лишь один вид НС, например, зафиксируем конкретное значение i=1. Далее, количественные показатели НС, например, за μ лет сведем в Табл. 1, где - $f_i^{(j)}$, $j = \overline{1,\mu}$, μ - количество лет, $i = \overline{1,12}$, i – номер месяца в году.

Шаг 1.2. Исходя из данных Табл. 1, с помощью формулы (4) можно получить одну строку данных усредненных помесячных количественных значений НС по столбцам:

$$f_t^{уср} = \sum_{i=1}^{\mu} f_t^{(i)} / \mu, \; t = \overline{1,12}. \qquad (4)$$

Табл. 1. Количественные показатели НС ($f_i^{(j)}$), произошедших в течение последних μ лет по месяцам

t	1	2	3	4	5	6	7	8	9	10	11	12
1	$f_1^{(1)}$	$f_2^{(1)}$	$f_3^{(1)}$	$f_4^{(1)}$	$f_5^{(1)}$	$f_6^{(1)}$	$f_7^{(1)}$	$f_{18}^{(1)}$	$f_9^{(1)}$	$f_{10}^{(1)}$	$f_{11}^{(1)}$	$f_{12}^{(1)}$
⋮	…	…	…	…	…	…	…	…	…	…	…	…
μ	$f_1^{(\mu)}$	$f_2^{(\mu)}$	$f_3^{(\mu)}$	$f_4^{(\mu)}$	$f_5^{(\mu)}$	$f_6^{(\mu)}$	$f_7^{(\mu)}$	$f_8^{(\mu)}$	$f_9^{(\mu)}$	$f_{10}^{(\mu)}$	$f_{11}^{(\mu)}$	$f_{12}^{(\mu)}$

Табл. 2. Усредненная строка количественных показателей произошедших НС

t	1	2	3	4	5	6	7	8	9	10	11	12
f_t^{ycp}	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}

Табл. 3.Усредненная строка количественных показателей произошедших НС, округленных до целого относительно данных Табл. 2

t	1	2	3	4	5	6	7	8	9	10	11	12
f_{ut}^{ycp}	f_{u1}	f_{u2}	f_{u3}	f_{u4}	f_{u5}	f_{u6}	f_{u7}	f_{u8}	f_{u9}	f_{u10}	f_{u11}	f_{u12}

Аналогичные таблицы желательно построить относительно других существенных видов НС.

Шаг 1.3. Для дальнейших расчетов необходимо подготовить данные, которые являются данными округленными до целого относительно данных Табл. 2 и Табл. 3.

Шаг 1.4. Применительно к усредненным данным можно построить математическую модель в форме пространства состояний (ПС) по методике, изложенной в [3]:

$$x(t+1) = a \cdot x(t) + b + w(t), \quad x(1) = \bar{x}_1, \quad (5)$$

$$f^{ycp}(t+1) = x(t+1) + v(t+1), \quad t = \overline{1, N-1}. \quad (6)$$

где $x(t)$ – истинное количество фиксированного вида НС, произошедших в течение месяца t; $w(t)$ – белое гауссовское ненаблюдаемое воздействие на зафиксированный вид НС в момент времени t с нулевым математическим ожиданием и неизвестной дисперсией Q; $x(1)$ – гауссовская величина, отражающая количество НС в начальный в момент времени $t = 1$ с математическим ожиданием $\bar{x}_1$ и неизвестной дисперсией $P(1)$; a, b – неизвестные коэффициенты в модели динамики (5); t – номер месяца в году; $N = 12$ – число месяцев в году; $f_t^{ycp} = f^{ycp}(t)$ – наблюдаемое случайное количество НС в течение месяца t (данные из репозитория SIEM-системы или из журнала наблюдений предприятия); $v(t)$ – белая гауссовская последовательность ошибок наблюдений относительно количества НС в течение каждого месяца с нулевым математическим ожиданием и неизвестной дисперсией R.

На данном шаге требуется оценить все дисперсии, связанные с шумами модели динамики $\hat{Q}$ и шумом величины начального состояния $\hat{P}(1)$, шумами измерительной системы $\hat{R}$ на основе выхода данных наблюдений и рекуррентных формул, которые приведены в работе [3].

Шаг 1.5. Оценки коэффициентов $\hat{a}, \hat{b}$ в модели динамики (5) можно рассчитать с помощью метода наименьших квадратов (МНК) на основе (возможно отфильтрованных от шумов) данных наблюдений $\left\{x(t) \approx f^{ycp}(t), t = \overline{1, N}\right\}$.

Шаг 1.6. Построенная модель ПС (5), (6) позволит получить наиболее достоверные оценки количества НС (в режиме реального времени с помощью уравнений фильтра Калмана), относительно каждого месяца в виде оценок фильтрации за последующий, например, (μ +1) год. Полученные оценки фильтрации должны быть округлены до ближайшего целого.

Шаг 1.7. Оценки фильтрации за 12 месяцев (μ +1) года (рассчитанные на основе данных реальных наблюдений и оценок предсказаний) позволят рассчитать объективные вероятностные оценки реализаций НС. Например, предлагается следующая процедура расчета вероятности для конкретного вида НС.

Пусть нас интересует вероятность появления НС в каждом месяце предыдущего μ-го года. Для этого подсчитывается общее суммарное количество (для усредненного количества) НС оценок фильтрации в течение всего μ-года ($F^{(\mu)}$), а затем фильтрационная оценка количества НС

Табл. 4. Объективные вероятности $(p_t^{(\mu)})$ реализаций конкретного вида НС в течение μ-го года

t	1	2	3	4	5	6	7	8	9	10	11	12
$p_t^{(\mu)}$	$p_1^{(\mu)}$	$p_2^{(\mu)}$	$p_3^{(\mu)}$	$p_4^{(\mu)}$	$p_5^{(\mu)}$	$p_6^{(\mu)}$	$p_7^{(\mu)}$	$p_8^{(\mu)}$	$p_9^{(\mu)}$	$p_{10}^{(\mu)}$	$p_{11}^{(\mu)}$	$p_{12}^{(\mu)}$

в течение каждого месяца ($f^{(\mu)}(t)$) делится на общую суммарную оценку фильтрационных оценок количества НС ($F^{(\mu)}$) в течение одного μ-года, которая определяется по формуле (Табл.4):

$$p^{(\mu)}(t) = f^{(\mu)}(t) / F^{(\mu)}, \quad t = \overline{1,12}, \qquad (7)$$

где $p_t^{(\mu)} = p^{(\mu)}(t)$ – объективная вероятность реализации конкретного вида НС в течение каждого месяца μ-года и всех 12 месяцев. При этом для μ-го года будем иметь:

$$\sum_{t=1}^{12} p^{(\mu)}(t) = 1, \quad \mu = 4, 5, \ldots .$$

где $p_t^{(\mu)}$, $t = \overline{1,12}$, μ-ый - год.

Алгоритм 1 апробирован на тестовом примере, который описан в работе [3].

1.2. Объективная стоимостная оценка предсказания величины ущерба от нарушений безопасности ИР

Алгоритм 2

Шаг 2.1. Пусть $O = \{O_i, i = \overline{1,m}\}$ – множество видов НС, приводящих к нарушению безопасности ИР. Выше была предложена процедура расчета оценки помесячной объективной вероятности количества нарушений определенного вида атаки на ИР в ИС предприятия. Предположим, что в отделе информационной безопасности (ИБ) предприятия или в репозитории SIEM-системы имеется статистика относительно ежемесячной оценки ущерба, которая соответствует ежемесячному количеству нарушений ИБ конкретного i-го вида атаки, т.е. значениям данных Табл. 1 соответствуют значения данных Табл. 5, где - $S_i^{(j)}$, $j = \overline{1,\mu}$, μ - количество лет, $i = \overline{1,12}$, i – номер месяца в году. Пусть, например, $i = 1$.

Шаг 2.2. Заметим, что не всегда ежемесячные показатели ущерба прямо пропорциональны количеству произошедших НС. Тем не менее, на основе данных Табл. 5 можно построить линейную модель в форме ПС, которая будет соответствовать усредненным данным наблюдений по столбцам относительно данных Табл. 5. Элементы строки усредненных данных вычисляются с помощью соотношения (8) (Табл. 6):

$$s_t^{(y)} = (\sum_{t=1}^{\mu} S_t^{(\mu)}) / \mu, \; t = \overline{1,12}. \qquad (8)$$

Шаг 2.3. На основе строки усредненных данных $\{s_t^{(y)}, \; t = \overline{1,12}\}$ по алгоритму, описанному в работах [3] можно построить линейную модель в форме ПС вида:

$$s(t+1) = \hat{c} \cdot s(t) + \hat{d} + w(t), \quad s(0) = s_0, \quad t = \overline{0,11}, \; (9)$$

$$s^y(t+1) = s(t+1) + v(t+1), \quad t = \overline{0,11}. \qquad (10)$$

При этом сначала на основе строки усредненных данных соответствующих таблице ущербов рассчитываются оценки неизвестных дисперсий шумов модели вида (9), (10), а именно оценки дисперсий $\hat{Q}$, $\hat{R}$, $\hat{P}(1)$ на основе рекуррентных формул, которые предложены в [3].

Табл. 5. Количественные ежемесячные показатели ущерба $(S_i^{(j)})$ от нарушений ИБ в зависимости от *i*-го вида атаки

t	1	2	3	4	5	6	7	8	9	10	11	12
1	$S_1^{(1)}$	$S_2^{(1)}$	$S_3^{(1)}$	$S_4^{(1)}$	$S_5^{(1)}$	$S_6^{(1)}$	$S_7^{(1)}$	$S_8^{(1)}$	$S_9^{(1)}$	$S_{10}^{(1)}$	$S_{11}^{(1)}$	$S_{12}^{(1)}$
⋮	…	…	…	…	…	…	…	…	…	…	…	…
μ	$S_1^{(\mu)}$	$S_2^{(\mu)}$	$S_3^{(\mu)}$	$S_4^{(\mu)}$	$S_5^{(\mu)}$	$S_6^{(\mu)}$	$S_7^{(\mu)}$	$S_8^{(\mu)}$	$S_9^{(\mu)}$	$S_{10}^{(\mu)}$	$S_{11}^{(\mu)}$	$S_{12}^{(\mu)}$

Табл. 6. Усредненная строка ежемесячных количественных показателей ущерба $s_t^{(y)}$

t	1	2	3	4	5	6	7	8	9	10	11	12
$s_t^{(y)}$	$s_1^{(y)}$	$s_2^{(y)}$	$s_3^{(y)}$	$s_4^{(y)}$	$s_5^{(y)}$	$s_6^{(y)}$	$s_7^{(y)}$	$s_8^{(y)}$	$s_9^{(y)}$	$s_{10}^{(y)}$	$s_{11}^{(y)}$	$s_{12}^{(y)}$

Шаг 2.4. Далее рассчитываем коэффициенты $\hat{c}, \hat{d}$ модели динамики (9) с помощью МНК на основе данных Табл. 6.

Шаг 2.5. Предположим, что мы располагаем данными наблюдений количественных показателей ущерба (например, из SIEM-системы), нанесенных ИР предприятия в $(\mu+1)$ году. См. Табл. 7, где - $S_t^{(\mu)}$, $t=\overline{1,12}$, $\mu=\mu+1$ -ый - год.

Используя уравнения фильтра Калмана и данные Табл. 7, получим последовательность оценок фильтрации $\left\{\hat{s}(t\,|\,t), t=\overline{1,12}\right\}$ относительно ежемесячных более достоверных количественных показателей нанесенного ущерба (Табл. 8).

Шаг 2.6. Используя округленные до ближайших целых чисел данные оценок фильтрации относительно количественных показателей, свершившихся НС в течение $(\mu+1)$ года по месяцам (данные Табл.3 и 8) относительно оценок фильтрации как количественных показателей ущерба, нанесенных на ИР предприятия в $(\mu+1)$ году, можно получить усредненный ущерб нанесенных от единичного случая свершившегося НС $\left\{e(t),\ t=\overline{1,12}\right\}$. Для этого необходимо данные строки Табл. 8 разделить на соответствующие данные из Табл. 3, округленные до целого, элементы строки данных количества реализации НС. Расчетные данные можно свести в Табл. 9.

Шаг 2.7. Предсказывая количество НС (f_i^{pre}) i-го вида с помощью соответствующей модели в форме ПС (5), (6) и соответствующего усредненного ущерба от единичного случая свершившегося НС (т.е. по данным Табл. 9), можно получить оценку предсказания величины ущерба, которая будет нанесена предприятию в t - ый месяц $(\mu+2)$ текущего года.

Алгоритм 2 апробирован на тестовом примере, который описан в работе [3].

1.3. Группы контролей безопасности

Меры безопасности (альтернативное название - "контроли безопасности"), возможно применяемые в организации для ИБ в ИС предприятия, можно поделить на три основные группы: технические, операционные и управленческие [7]. Группы в свою очередь разбиваются на семейства. Перечислены эти меры безопасности в стандарте [10].

В группу управленческих контролей входят меры безопасности для ИС, которые используются для управления рисками и ИБ ИС. Группа содержит пять семейств контролей [7, 10]. В группу операционных контролей входят меры безопасности для ИС, которые, прежде всего, реализуются и выполняются людьми. В группу входят 9 семейств контролей. В группу технических контролей входят меры безопасности для ИС, которые, прежде всего, реализуются и выполняются через действия в аппаратных средствах, программном обеспечении системы. В группу входят четыре семейства контролей [7, 10].

Эксперты, которые проводят оценки риска, могут приходить с различной профессиональной подготовкой, например: технической, финансовой, инженерной и управленческой, со своими собственными индивидуальными восприятиями, отношениями и побуждениями в определении ущерба от количества реализованных НС. Поэтому перед началом расчета величины риска в ИС предприятия на основе

Табл. 7. Ежемесячные количественные показатели ущерба от нарушений ИБ в зависимости от i - го вида атаки в $(\mu+1)$ году

t	1	2	3	4	5	6	7	8	9	10	11	12
$S_t^{(\mu)}$	$S_1^{(\mu)}$	$S_2^{(\mu)}$	$S_3^{(\mu)}$	$S_4^{(\mu)}$	$S_5^{(\mu)}$	$S_6^{(\mu)}$	$S_7^{(\mu)}$	$S_8^{(\mu)}$	$S_9^{(\mu)}$	$S_{10}^{(\mu)}$	$S_{11}^{(\mu)}$	$S_{12}^{(\mu)}$

Табл. 8. Ежемесячные количественные показатели оценок фильтрации нанесенного ущерб в $(\mu+1)$ году

t	1	2	3	4	5	6	7	8	9	10	11	12
$\hat{s}(t\,|\,t)$	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	s_{12}

Табл. 9. Усредненный нанесенный ущерб от единичного случая свершившегося НС

t	1	2	3	4	5	6	7	8	9	10	11	12
$e(t)$	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}

экспертных оценок необходимо всем экспертам ознакомиться со всеми объективными оценками предсказания и фильтрации, имеющихся в отделе ИБ предприятия либо в репозитории SIEM-системы, относительно ежемесячных количеств НС и ущерба от реализованных НС, которые позволят экспертам наиболее реалистично и достоверно предлагать последующие экспертные оценки.

После ознакомления с объективными вероятностными оценками количества НС и оценками ущербов, процедура оценки риска на основе экспертных оценок организовывается с помощью следующих шести этапов [7]: Характеристика Системы; Идентификация Угроз и Уязвимостей; Оценка Вероятности; Анализ Последствия; Определение Риска; Рекомендации по Управлению.

Например, пусть на предприятии, для которого мы оцениваем риски, существует три ИС: ИС-1, ИС-2, ИС-3. Экспертами после ознакомления с результатами объективных оценок были обнаружены определенные уязвимости и угрозы, относящиеся к различным семействам контролей. Далее были проведены расчеты экспертных оценок по методике, описанной в работе [7]. Исходные тестовые данные и численные расчеты приведены в работе [3].

После ранжирования ИС по уровню риска в порядке убывания были получены расчетные данные, показанные в Табл. 10.

Из таблицы видно, что ИС-2 получает самый высокий уровень риска. Значит, вероятность реализации угроз и ущерб для этой системы больше, чем для остальных. Поэтому руководителям организации, в первую очередь, необходимо обратить внимание на безопасность ИС-2. Более подробную детальную рекомендацию можно получить от соответствующих узлов SIEM-систем.

Табл.10. Ранги информационных систем

Информационная система	ИС-2	ИС-3	ИС-1
Уровень риска	0,453	0,446	0,410

1.4. Алгоритм фильтра Калмана. Случай взаимно-коррелированных шумов динамики и измерителя

Выше было отмечено примерное содержание основных механизмов по уровням иерархии SIEM-системы:

- нормализация означает приведение форматов записей журналов, собранных из различных источников к единому внутреннему формату;
- корреляция разнородных событий;
- анализ событий, инцидентов и их последствий, включающая процедуры моделирования событий;
- анализ уязвимостей и защищенности системы;
- оценка риска с учетом корреляций шумов поведения динамики исследуемого объекта и шумов данных наблюдений, которые могут быть использованы при построении модели в форме ПС для расчетов оценок предсказания и оценок фильтрации.

В Алгоритмах 1 и 2 при построении моделей в форме ПС предполагалось, что шумы динамики и измерительной системы - белые и гауссовские. Эти шумы между собой и начальным состоянием предполагались взаимно-некоррелированными. При этих условиях для расчетов оценок предсказаний и фильтраций использовались стандартные уравнения фильтра Калмана.

Но на практике могут встречаться случаи, когда шумы динамики и измерительной системы могут быть взаимно-коррелированными. Поэтому в данном разделе рассматривается алгоритм фильтра Калмана, как вариант расширения соответствующего узла SIEM-системы, дополнительным алгоритмом для случая, когда шумы динамики и измерителей коррелированы между собой.

Пусть объект исследования описывается стационарными непрерывно-дискретными моделями в форме ПС вида:

$$\dot{x}(t) = A \cdot x(t) + B + C \cdot w(t),\ x(t_0) = x_0, \qquad (11)$$

$$y(t_k + 1) = H \cdot x(t_k) + v(t_k), t_{k-1} \le t \le t_k, k = \overline{1, N}, \qquad (12)$$

где $x - n-$вектор состояния; $\dot{x} - n-$вектор производной состояния по времени $t \ge t_0$; $w - q-$ вектор шумов динамики; $y - m-$вектор наблюдений; $v - m-$вектор шумов измерителей.

Предполагается, что система представляет собой стационарный процесс. Поэтому матрицы A, B, C являются постоянными и имеют размеры $n \times n$, $n \times r$, $n \times q$. Непрерывное время обозначается символом t, производная по

времени - точкой сверху, а дискретное время - через t_k. Нижний индекс отмечает порядковый номер момента времени наблюдения. Случайный процесс $\{w(t), t \geq t_0\}$ представляет собой белый гауссовский шум с нулевым математическим ожиданием и матричной корреляционной функцией вида:

$$E[w(t)w^T(\tau)] = Q \cdot \delta(t-\tau), \text{ для всех } t, \tau \geq t_0,$$

где $\delta(t-\tau)$ - дельта функция Дирака.

Матрица Q размера $q \times q$ непрерывна и неотрицательно определена для $t \geq t_0$.

Последовательность $\{v(t_k), t_k \in [t_0, t_N], k = 0, 1, 2, \ldots, N\}$ представляет собой белую гауссовскую последовательность с нулевым математическим ожиданием и матричной корреляционной функцией вида:

$$E[v(t_k) \cdot v^T(\tau_j)] = R \cdot \delta_{kj},$$

где δ_{kj} – символ Кронекера, значения которого определяются из соотношения $\delta_{kj} = \begin{cases} 1 & при \quad k = j, \\ 0 & при \quad k \neq j, \end{cases}$ для всех $t_k, \tau_j \geq t_0$.

Матрица R размера $m \times m$ положительна определена для $t_k \geq t_0$. Предполагается также, что два указанных в (11), (12) случайных процесса в дискретном представлении $w(t_k)$ и $v(t_j)$ коррелированы между собой:

$$E\left[\left(\frac{w(t_k)}{v(t_k)}\right) \cdot \left(w^T(t_k) \vdots v^T(t_k)\right)\right] = \begin{pmatrix} \tilde{Q} & S \\ S^T & R \end{pmatrix}$$

для всех $t_k \geq t_0$, при $\tilde{Q} \geq 0,\ S \geq 0,\ R > 0,$

где S – взаимно-корреляционная матрица шумов динамики объекта и измерителя размера $q \times m$; $\tilde{Q}$ - ковариационная матрица для дискретной модели, соответствующая непрерывной модели.

При этом для оценок состояния линейной непрерывно-дискретной системы будем использовать результаты работы [11], в которой алгоритм оценивания состояния для линейных дискретных систем обобщается на случай взаимно-коррелированных шумов объекта и измерителя.

При предположениях, указанных выше, оценки состояния будут вычисляться по следующим формулам (для непрерывной обновленной последовательности):

$$\dot{\hat{x}}(t \mid t_k) = A \cdot \hat{x}(t \mid t_k) + B + F_0(t) \cdot \tilde{y}(t_k); \quad \hat{x}(t_0 \mid t_0) = x(t_0); \tag{13}$$

$$\dot{P}(t \mid t_k) = A_0 \cdot P(t \mid t_k) + P(t \mid t_k) \cdot A_0^T + Q_0; \quad P(t_0 \mid t_0) = P(t_0); \tag{14}$$

$$K(t_{k+1}) = P(t_{k+1} \mid t_k) \cdot H^T \cdot [H \cdot P(t_{k+1} \mid t_k) \cdot H^T + R]^{-1}; \tag{15}$$

$$\hat{x}(t_{k+1} \mid t_{k+1}) = \hat{x}(t_{k+1} \mid t_k) + K(t_{k+1}) \cdot [y(t_{k+1}) - H \cdot \hat{x}(t_{k+1} \mid t_k)]; \tag{16}$$

$$P(t_{k+1} \mid t_{k+1}) = [I - K(t_{k+1}) \cdot H] \cdot P(t_{k+1} \mid t_k); \tag{17}$$

где $A_0 = A - F_0 \cdot H; \quad F_0 = C \cdot S \cdot R^{-1};$ $Q_0 = C \cdot Q \cdot C^T - F_0 \cdot R \cdot F_0^T$ при $t_k \geq t_0,\ k = 0, 1, 2, \ldots, N,$ $t_1 \leq t \leq t_N$.

Как видим структура алгоритмов фильтрации при взаимно-коррелированных шумах объекта и измерителя почти аналогичны алгоритму фильтрации при взаимно-некоррелированных шумах. Существенным отличием является запись дифференциального уравнения (13) для оценок предсказания. Это уравнение содержит дополнительное слагаемое, учитывающее информацию о коррелированности шумов, и которое требует на первом этапе знания наблюдения для начального состояния объекта. Этот вопрос в работе [11] остается открытым. Нужно заметить, что эта проблема возникает лишь в том случае, когда шумы коррелированны. Здесь, видимо, можно предложить два способа оценки наблюдения для состояния в момент запуска объекта. Первый способ состоит в том, что мы для достаточно малых временных интервалов проводим серию наблюдений и, предполагая, что шумы некоррелированные и используя алгоритм фильтрации при некоррелированных шумах, определяем серию оценок предсказания наблюдений. Затем производим по этим известным оценкам наблюдений предсказания на один шаг назад. На практике можно столкнуться со случаями, когда связь между шумами объекта и измерителя тесная, тогда вышеизложенный способ может привести к плохой оценке наблюдения для начального состояния объекта. В этом случае, видимо, проще использовать уравнения наблюдения для оценки в момент запуска системы.

Информация о взаимной корреляции шумов динамики и измерительной системы содержится также в уравнении (14), тогда как уравнение расчета корреляционной матрицы ошибки оценок предсказания в стандартных уравнениях фильтра Калмана такого слагаемого не содержит.

2. Оценивание эффективности инвестиций и оптимальный выбор средств для комплексной системы защиты информации

2.1. Анализ защищенности информационных ресурсов предприятия

Состояние защищенности ИР предприятия не является постоянным и находится в прямой зависимости от уровня технического, программного, экономического развития, прибыли (дохода), стоимости материальных ценностей предприятия. При этом существуют следующие связи [12, 13]:

- увеличение объема прибыли, материальных ценностей влечет необходимость повышения уровня защищенности ИР;
- с увеличением величины прибыли возрастает число угроз ИБ;
- увеличение числа угроз и появления новых уязвимостей вызывает необходимость улучшения качества защиты информации на предприятии;
- для повышения уровня защищенности ИР и информации увеличивают затраты на ее защиту;
- увеличение уровня защиты информации предприятия снижает уровень воздействия угроз.

Таким образом, состояние защищенности ИР предприятия находится в объективной связи как с уровнем технического, программного, экономического развития, так и с возможностями угроз по нанесению ему материального ущерба.

Если относиться к вложениям в ИБ как к затратам, то их сокращение позволит решить тактическую задачу освобождения средств. Однако это заметно отдалит компанию от решения стратегической задачи. Поэтому, если у компании есть долгосрочная стратегия развития, она рассматривает вложения в ИБ как инвестиции. Именно такой подход позволяет определить цели и задачи построения комплексной, активной системы защиты информации [13] с элементами интеллектуальных сервисов [1, 2], предусмотренных в SIEM-системах.

2.2. Оптимальный выбор средств комплексной системы защиты информации от возможных угроз ИБ

Специалисты в области ИБ предлагают различные методы оценки эффективности инвестиций в систему ИБ. Например, в [13] автор описывает подход к оценке эффективности управления рисками, который подразумевает вложение инвестиций. Для построения экономически эффективной системы защиты необходимо решить задачу оптимального выбора средств реализации системы защиты ИР от комплекса возможных угроз информации [14]. Такие задачи необходимо решать, опираясь на существующие математические аппараты, например, можно использовать методы теории игр [4, 15].

Теория игр предполагает наличие продавца и покупателя. Матричная игра, когда игрок взаимодействует с окружающей средой, решает задачу определения наиболее выгодного варианта поведения с учетом неопределенности состояния окружающей среды и которая называется статистической игрой. Игрок в таком случае называется лицом, принимающим решение (ЛПР) [15].

2.2.1. Постановка задачи

Взаимосвязь между продавцом и покупателем определяется платежной матрицей. В общем виде платежная матрица статистической игры состоит из: строк A_i – стратегии ЛПР; столбцов матрицы S_j – состояния окружающей среды, $\{ w_{ij}, i = \overline{1,m}, j = \overline{1,n} \}$ – ожидаемый выигрыш при использовании стратегии A_i в случае, если среда находится в состоянии S_j.

В практике принятия решений, ЛПР руководствуется следующими возможными критериями: Вальда, Гурвица, Сэвиджа и др. [15]. В нашем случае, когда необходимо выбрать средство защиты информации в зависимости от различных типов атак, будем осуществлять выбор согласно критерию Вальда. Критерий Вальда обеспечивает выбор осторожной пессимистической стратегии в той или иной деятельности. Для каждого решения выбирается самая

Табл. 11. Вероятности отражения атаки

Группы атак		Средства защиты			
		S_1	S_2	…	S_n
		Вероятности отражения атаки			
	A_{11}	$p^{(з)}_{111}$	$p^{(з)}_{112}$	…	$p^{(з)}_{11n}$
	…	…	…	…	…
	A_{1r_1}	$p^{(з)}_{1r_11}$	$p^{(з)}_{1r_12}$	…	$p^{(з)}_{1r_1n}$
	…	…	…	…	…
	A_{mr_m}	$p^{(з)}_{mr_m1}$	$p^{(з)}_{mr_m2}$	…	$p^{(з)}_{mr_mn}$

Табл. 12. Стоимость средств защиты X_j, $j = 1, 2, 3, ..., n$

Средства защиты	S_1	S_2	…	S_n
Стоимость средств защиты	X_1	X_2	…	X_n

худшая ситуация (наименьшее из w_{ij}) и среди них отыскивается гарантированный максимальный эффект:

$$W = \max_j \min_i w_{ij},\ i = \overline{1,m},\ j = \overline{1,n}.$$

Можно принять и критерий выбора оптимистической стратегии:

$$W = \min_i \max_j w_{ij},\ i = \overline{1,m},\ j = \overline{1,n},$$

где оценивается гарантированный выигрыш при самых благоприятных условиях.

В критерии Гурвица происходит ориентация на самый худший исход, что является своеобразной подстраховкой. Однако опрометчиво выбирать политику, которая излишне оптимистична. Критерий Гурвица предлагает некоторый компромисс:

$$W = \max[\alpha \max W_{ij} + (1-\alpha)\min W_{ij}],$$
$$i = \overline{1,m},\ j = \overline{1,n}, \qquad (18)$$

где параметр α принимает значение от 0 до 1 и выступает как коэффициент оптимизма.

Допустим, известны следующие показатели: A_{ir_i} – группы атак; m – количество групп атак $\{ i = \overline{1,m} \}$; r_i – количество атак в группе i; $\{ S_j,\ j = \overline{1,n} \}$ – средства защиты; n – количество средств защиты; $X_1, X_2, \ldots, X_n$ – стоимость применяемого средства защиты; Y – величина предполагаемого ущерба; w_{ir_ij} или $\{ p^{(3)}_{ir_ij};\ i = \overline{1,m},\ j = \overline{1,n} \}$ – вероятность защиты, т.е. вероятность отражения атаки A_{ir_i} при использовании средства защиты S_j; $p^{(a)}_{ir_i}$ – вероятность проведения атаки; $p^{(y)}_{ir_ij}$ – вероятность нанесения ущерба при i-ой атаке и j-м средстве защиты с учетом частоты использования i-й атаки.

В соответствии с видом платежной матрицы представим вероятности отражения атаки в Табл. 11.

Как правило, ни одно из средств защиты не обеспечивает ее на 100%, поэтому вероятности отражения атак будут строго меньше 1. В Табл. 12 представлена стоимость средств защиты.

Необходимо отметить, что неограниченное вложение денежных средств не означает гарантированную защиту ИР. Условием эффективной защиты является следующее правило: стоимость средств защиты должна быть меньше стоимости потерь, понесенных при успешной реализации атаки. Все статистические данные могут быть взяты из отдела ИБ предприятия или репозитория в соответствующих узлах SIEM-систем.

2.2.2. Методика решения задачи

Утверждение. Критерий «стоимость-эффективность»: общая стоимость средств защиты должна быть меньше стоимости потерь, понесенных при успешной реализации атак. Математическое выражение критерия «стоимость-эффективность» будет соответствовать неравенству:

$$\lambda_{ir_ij} = \frac{X_j}{(1 - p^{(3)}_{lr_ij}) \times p^{(a)}_{ir_i} \times Y} \le 1;\ i = \overline{1,m},\ j = \overline{1,n}. \qquad (19)$$

Табл. 13. Матрица коэффициентов эффективной защиты при величине предполагаемого ущерба Y с выбором средства эффективной защиты

Атаки	Вероятность использования злоумышленником различных групп атак	Средства защиты			
		S_1	S_2	…	S_n
		Коэффициенты эффективной защиты			
A_{11}	$p_{11}^{(a)}$	λ_{111}	λ_{112}	…	λ_{11n}
…	…	…	…	…	…
A_{1r_1}	$p_{1r_1}^{(a)}$	λ_{1r_11}	λ_{1r_12}	…	λ_{1r_1n}
A_{21}	$p_{21}^{(a)}$	λ_{211}	λ_{212}	…	λ_{21n}
…	…	…	…	…	…
A_{m1}	$p_{m1}^{(a)}$	λ_{m11}	λ_{m12}	…	λ_{m1n}
…	…	…	…	…	…
A_{mr_m}	$p_{mr_m}^{(a)}$	λ_{mr_m1}	λ_{mr_m2}	…	λ_{mr_mn}

Доказательство. Вероятность того, что мы применим одно из средств защиты равна 1 (100%). Составим следующее неравенство:

$$1 \times X_j \le p_{ir_ij}^{(y)} \times Y;\ i = \overline{1,m},\ j = \overline{1,n}. \qquad (20)$$

Представим вероятность нанесения ущерба $p_{lr_ij}^{(y)}$ через вероятность защиты от атаки ($p_{lr_ij}^{(3)}$) и вероятность проведения атаки ($p_{lr_i}^{(a)}$):

$$p_{ir_ij}^{(y)} = (1 - p_{lr_ij}^{(3)}) \times p_{ir_i}^{(a)};\ i = \overline{1,m},\ j = \overline{1,n}. \quad (21)$$

Подставив (21) в (20), получим:

$$X_j \le (1 - p_{lr_ij}^{(3)}) \times p_{ir_i}^{(a)} \times Y;\ i = \overline{1,m},\ j = \overline{1,n}. \quad (22)$$

Разделив обе части соотношения (22) на выражение, стоящее в правой части этого неравенства, получим:

$$\frac{X_j}{(1 - p_{lr_ij}^{(3)}) \times p_{ir_i}^{(a)} \times Y} \le 1\ ;\ i = \overline{1,m},\ j = \overline{1,n}. \quad (23)$$

Обозначим в (23) левую часть неравенства через λ_{ir_ij} и назовем коэффициентом эффективной защиты:

$$\lambda_{ir_ij} = \frac{X_j}{(1 - p_{lr_ij}^{(3)}) \times p_{ir_i}^{(a)} \times Y};\ i = \overline{1,m},\ j = \overline{1,n}.$$

Учитывая нестрогое неравенство (23) приходим к выводу, что математическим выражением условия эффективной защиты будет соотношение:

$$\lambda_{ir_ij} \le 1;\ i = \overline{1,m},\ j = \overline{1,n} \qquad (24)$$

что и требовалось доказать.

Коэффициенты эффективной защиты представлены в Табл. 13.

Условие (24) будем использовать наряду с критерием Вальда. Правило выбора решения в соответствии с максиминным критерием Вальда можно интерпретировать следующим образом. Платежная матрица Табл. 13 дополняется строкой, каждый элемент которой представляет собой минимальное значение выигрыша в соответствующей стратегии ЛПР (при этом пусть $k = r_1 + r_2 + \cdots + r_m + 1$):

$$W_{kj} = \min w_{ij},\ i = \overline{1,m},\ j = \overline{1,n}.$$

Оптимальной по данному критерию считается та стратегия ЛПР, при выборе которой минимальное значение выигрыша максимально:

$$W = \max W_{kj},\ k = r_1 + r_2 + \cdots + r_m + 1,\ j = \overline{1,n}.$$

Выбранная, таким образом, стратегия полностью исключает риск. Это означает, что принимающий решение не может столкнуться с худшим результатом, чем тот, на который он ориентируется.

Предложенная выше методика апробирована на тестовом примере и описана в работе [3].

Заключение

Выше были даны: систематизированное изложение математических методов и моделей анализа мер безопасностей, которые были нацелены на изучение теоретических подходов для защиты ИР в КС; сформулированы и показаны практические навыки их разработки и

применение к расчету рисков относительно исследуемых информационных рисков.

Управления рисками основаны, прежде всего, на статистических данных, которые фиксируются, накапливаются, анализируются, хранятся, обрабатываются для оценивания потенциального ущерба от ошибок пользователей и атак нарушителей на ИР в ИС предприятия или в репозитории SIEM-систем. А также выбора мер для его минимизации, расчета оценок предсказания и фильтрации всех возможных параметров и показателей, связанных с ИБ. В частности, были предложены методики, позволяющие получать оценки объективной вероятности в возможности наступления НС, оценки объективной стоимости ущерба от нарушений безопасности ИР в ИС предприятия и оценки предсказания и фильтрации величины ущерба. Все основные расчеты показателей ИБ в ИС предприятия использовали возможности линейной стохастической модели в форме ПС и уравнений фильтра Калмана для получения более достоверных значений оценок состояния исследуемого объекта.

В работе сконцентрированы те методы и модели, которые наиболее часто используются для анализа и выработки решений о рациональном выборе и распределении мер безопасности относительно ИР. В процессе оценки рисков учитываются взаимозависимости между мерами безопасности, что позволяет расставить приоритеты в реализации мер безопасности, разработать адекватную стратегию управления рисками.

В работе приведено полученное авторами математическое выражение условия эффективной защиты, которое основывается на критерии «стоимость-эффективность». Приведенное условие эффективной защиты используется наряду с критериями Вальда и Гурвица. Согласно этому условию и критериям Вальда и Гурвица в расчетной части выявлена зависимость стоимости средств защиты от величины предполагаемого ущерба.

Литература

1. Котенко И.В., Саенко И.Б. SIEM-системы для управления информацией и событиями безопасности // Защита информации. INSIDE. 2012. № 5. С. 54-65.
2. Miller D.R., Harris Sh., Harper A.A. Van-Dyke S., Black Ch. Security Information and Event Management (SIEM) Implementation. McGrawHill Companies. 2011. - 430 p.
3. Абденов А.Ж., Заркумова-Райхель Р.Н. Оценивание риска в информационных системах на основе объективных и экспертных оценок // Вопросы защиты информации. 2015, № 1. – С. 64-70.
4. Абденов А.Ж., Заркумова Р.Н. Выбор средства эффективной защиты с помощью методов теории игр // Вопросы защиты информации. 2010, №2. – С. 26-31.
5. ISO/IEC 27005:2008. Information technology. Security techniques. Information security risk management. 2008. - 56 p.
6. Risk management: Implementation principles and inventories for risk management/risk assessment methods and tools. ENISA (European Network and Information Security Agency). 2006. - 168 p.
7. Chi-Chun Lo, Wan-Jia Chen. A hybrid information security risk assessment procedure considering interdependences between controls // Expert Systems with Applications. 2011. V.39. pp. 248-257.
8. Vose D. Risk Analysis: F Quantitative guide. 3-rd edition. John Wiley & Sons, 2008. - 752 p.
9. Kumamoto H., Henley E. Probabilistic risk assessment and management for engineers and scientists.2-nd edition. Institute of Electrical and Electronics Engineers. Inc. New York, 1996. - 620 p.
10. NIST SP 800-30:2012. Guide for conducting Risk Assessments // National Institute of Standards and Technology. – URL: http://csrc.nist.gov/publications/PubsSPs.html - 22 p.
11. Симкин М.М. О рекуррентной фильтрации при взаимно-коррелированных шумах объекта и измерителя//Автоматика и телемеханика, 1980, № 1, С. 71-80.
12. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии. – М.: Издательский центр «Академия». 2009. - 416 с.
13. Баранов Д. Оценка эффективности управления рисками // Информационная безопасность. 2004, № 2, июнь. – С. 26-27.
14. Теренин А.А. Проектирование экономически эффективной системы информационной безопасности // Защита информации. INSIDE. 2005, №1. – С. 26-35.
15. Оуэн Г. Теория игр. – М.: Мир. 1971. - 230 с.

Абденов Амирза Жакенович. Профессор кафедры "Информационные системы" Евразийского национального университета им. Л.Н. Гумилева, Астана, Республика Казахстан. Окончил Томский государственный университет в 1975 году. Доктор технических наук. Автор более 200 печатных работ и одной монографии. Область научных интересов: активная идентификация стохастических динамических систем, описываемых моделями в пространстве состояний; формализация решения задач в области информационной безопасности. E-mail: amirlan21@gmail.com

Трушин Виктор Александрович. Заведующий кафедрой "Защита информации" Новосибирского государственного технического университета. Окончил Новосибирский электротехнический институт в 1971 году. Кандидат технических наук. Автор более 100 печатных работ и трех монографий. Область научных интересов: решения задач в области технических средств защиты информации. E-mail: rastr89@mail.ru

Абденова Гаухар Амирзаевна. Старший преподаватель кафедры "Математического и компьютерного моделирования" Евразийского национального университета им. Л.Н. Гумилева, Астана, Республика Казахстан. Окончила Томский государственный университет в 1998 году. Кандидат технических наук. Автор более 35 печатных работ и одной монографии. Область научных интересов: идентификация стохастических динамических систем, решение задач в области математического моделирования экономических процессов. E-mail: gauhar76@ngs.ru

Иноземцева Юлия Александровна. Магистрант кафедры "Информационные системы" Евразийского национального университета им. Л.Н. Гумилева, Астана, Республика Казахстан. Окончила Евразийский национальный университет им. Л.Н. Гумилева в 2007 году. Автор двух печатных работ. Область научных интересов: формализация решения задач в области информационной безопасности. E-mail: yulia.inozemceva@gmail.com