УДК 004.056

И.Е. Горбачев, А.П. Глухов

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Горбачев И.Е., Глухов А.П. **Моделирование процессов нарушения информационной безопасности критической инфраструктуры.**

Аннотация. Рассматриваются принципы оценивания эффективности действий нарушителя в критической инфраструктуре. Представлен «операционный комплекс» моделирования процессов нарушения информационной безопасности. Исследованы неопределенности процесса моделирования нарушителя и пути их устранения. Разработана математическая модель агрегированного показателя эффективности действий нарушителя, которая снимает ряд ограничений существующих вероятностных моделей случайных явлений в области информационной безопасности. Модель носит название стохастического супериндикатора и предназначена для исследования конфликтных ситуаций в критической инфраструктуре.

Ключевые слова: критическая инфраструктура**,** информационная безопасность, операционный комплекс, модель нарушителя, процессы нарушения безопасности, показатель эффективности, стохастический супериндикатор.

Gorbachev I.E., Glukhov A.P. **Modeling of Processes of Information Security Violations of Critical Infrastructure.**

Abstract. Discusses the principles of evaluation the effectiveness of the malefactor in the critical infrastructure. The "operating complex" process modeling of security breach is presented. Investigated uncertainty modeling process of malefactor and ways to overcome them. A mathematical model of aggregate effectiveness of the malefactor, which removes some limitations of existing probabilistic models of random phenomena in the field of information security is developed. The model is called stochastic super indicator and is intended for research of conflict situations in critical infrastructure.

Keywords: critical infrastructure, information security, operating complex, model the malefactor, processes of a security breach, performance indicators, stochastic superindikator.

1. Введение. Информатизация критически важных объектов (КВО) на основе IP-технологии сделала обеспечение безопасности критической информационной инфраструктуры (КИИ) Российской Федерации (РФ) одной из наиболее острых проблем современности. Процесс информатизации обуславливает появление новых видов угроз информационной безопасности (ИБ), направленных, прежде всего, на системы управления и жизнеобеспечения КВО, которые наиболее подвергнуты деструктивным информационным воздействиям (ИВ). Повышенный уровень террористической угрозы в сочетании со стремительно возрастающим уровнем зависимости общества от промышленных систем требуют принятия скоординированных мер, направленных на снижение риска дезорганизации или полного прекращения функционирования КВО в условиях информационного конфликта. Одним из возможных направлений разрешения этой проблемы является проведение аудита ИБ КИИ КВО, основным

этапом которого является идентификация существующих угроз ИБ.

Актуальный перечень угроз ИБ должен определяться результатами моделирования возможных действий нарушителя ИБ КИИ. Согласно приказу ФСТЭК России от 14 марта 2014 г. N 31 [1], меры защиты информации, выбранные и реализованные в автоматизированных системах управления (АСУ) технологическим процессом (ТП) КВО, для АСУ 1, 2, 3 классов защищенности должны обеспечивать нейтрализацию угроз безопасности информации (УБИ) от нарушителя с высоким, не ниже среднего и низким потенциалами, соответственно.

В настоящее время не достаточна формализована методология оценивания уровня потенциала нарушителя и эффективности его ИВ. Фактически уровень определяется экспертно по известным только им критериям.

В статье рассмотрены следующие вопросы. Во втором разделе приведен краткий анализ нормативно-правовой базы РФ в данной предметной области. В третьем разделе рассматриваются особенности обеспечения ИБ КВО с учетом специфики АСУ ТП. Четвертый раздел посвящен разработке операционного комплекса моделирования процессов нарушения ИБ. В пятом разделе проведен анализ неопределенностей процесса моделировании нарушителя и оценивании эффективности его ИВ. В шестом разделе представлены рекомендации по моделированию нарушителя ИБ. В седьмом разделе раскрываются семантические аспекты исследования процессов нарушения ИБ и обосновывается показатель эффективности противодействия конфликтующих процессов – стохастический супериндикатор.

2. Анализ нормативно-правовой базы РФ, регламентирующей подходы к оцениванию уровня нарушителя ИБ. Подходы к оцениванию уровня опасности действий нарушителя ИБ в традиционных автоматизированных системах (АС) представлены на рисунке 1.

Классификация нарушителей ИБ (рисунок 1, первый подход) в настоящее время уже устарела, так как разрабатывалась без учета распределенной (сетевой) архитектуры современных АС. Второй подход (рисунок 1) позволяет классифицировать нарушителей ИБ не только по уровню полномочий доступа к защищаемой информации, но и учитывать сам факт наличия физического доступа в контролируемую зону предприятия. Однако данный подход оценивает нарушителя только по двум аспектам (в действительности их больше) и не позволяет с позиции квалиметрии измерить уровень потенциала нарушителя, а также оценить результативность его воздействий.

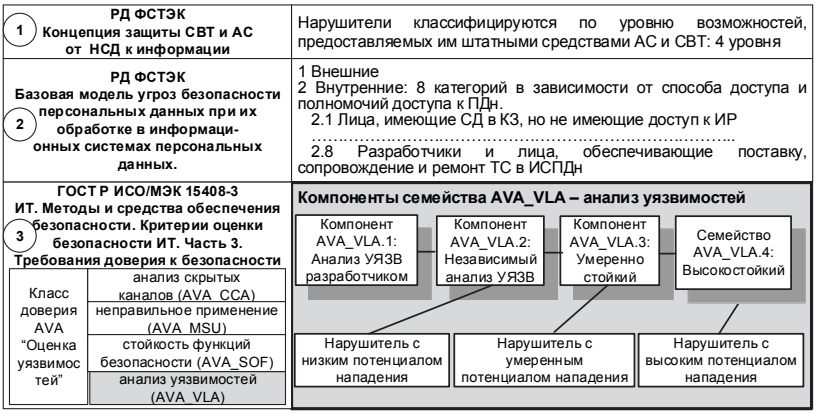

Рис. 1. Подходы к оцениванию уровня опасности действий нарушителя ИБ

В рамках подхода 3 (рисунок 1) предложено не ограничиваться рассмотрением способов взаимодействия нарушителя с объектом атаки и не делать никаких предположений относительно корректности реализации функций безопасности, а рассматривать ИВ исключительно в контексте результатов анализа уязвимостей АС. Основная цель этого анализа, проводимого в ходе аудита, – сделать заключение, что объект оценивания является стойким к нападению противника, обладающего низким, умеренным или высоким потенциалами нападения. Потенциал нарушителя должен определяться в ходе оценивания его возможностей, проводимого при определении актуальных угроз ИБ. Эти угрозы ИБ должны определяться по результатам моделирования возможных действий нарушителя, что требует произвести разработку методологических основ оценивания уровня потенциала нарушителя с учетом специфики АСУ ТП.

3. Особенности обеспечения ИБ КВО с учетом специфики АСУ ТП. В настоящее время становление направления, связанного с исследованием безопасности КВО, сдерживается отсутствием единых представлений о существе понятия ИБ АСУ ТП. Данные технологические системы имеют более высокие уровни риска по сравнению с традиционными АС, вплоть до нарушения работоспособности системы, выброса вредных веществ, техногенных катастроф и человеческих жертв. Поэтому помимо обеспечения конфиденциальности, целостности и доступности информации в первую очередь ставится вопрос о безопасности самого технологического процесса (ТП) в КВО.

На свойство безопасность ТП (рисунок 2) влияют элементарные свойства ТП и системы управления им – наблюдаемость, управляемость, идентифицируемость.

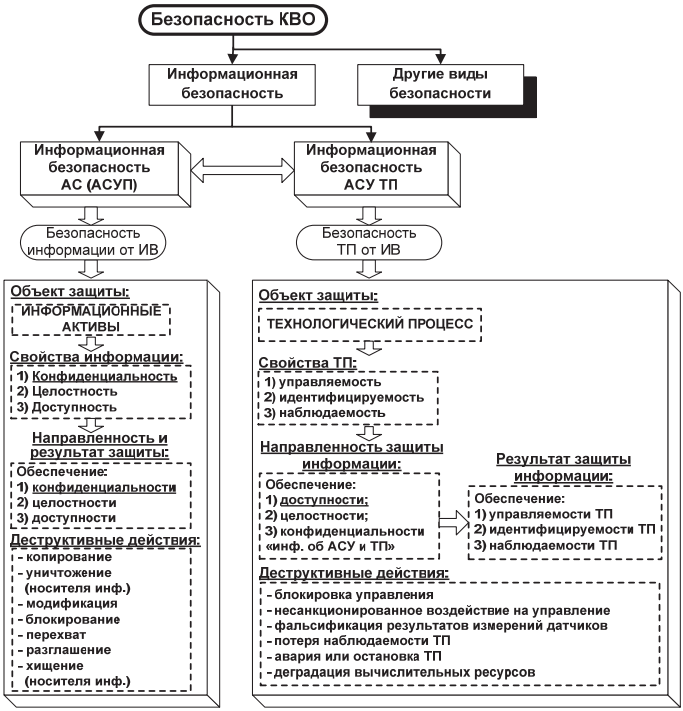

Рис. 2. Декомпозиция свойства безопасности АСУ ТП КВО

Поэтому целью защиты ТП является обеспечение требований управляемости, наблюдаемости и идентифицируемости ТП. При невыполнении этих требований возможны деструктивные действия на АСУ ТП, связанные с потерями:

- управляемости технологического процесса, включающей блокировку управления и/или несанкционированное управление;
- наблюдаемости технологического процесса: модификация параметров ТП и/или фальсификация измерений датчиков;
- работоспособности системы: авария (остановка) ТП и/или деградация вычислительных ресурсов.

Все деструктивные воздействия на АСУ ТП являются производными трех причин: нарушение доступности (отказ в обслуживании) критически важной информации, нарушение ее целостности (модифи-

кация) и конфиденциальности (утечки).

Критически важной информацией является закрепленная в документации на АСУ ТП «технологическую» информацию, уничтожение, блокирование или искажение которой может привести к нарушению функционирования АСУ ТП, а также информацию «об АСУ ТП и ТП», которая в случае ее хищения может быть использована для деструктивных информационных воздействий на АСУ ТП. «Технологической» информацией является:

- оперативная (динамическая) информация (телеметрия, телеизмерения, телеуправление) о протекании управляемого ТП;
- архивная (статическая) информация (нормативно-техническая документация, параметры ТП и другая архивная информация).

Под информацией «об АСУ ТП и технологическом процессе» понимается информация о составе, характеристиках управляемого процесса, характеристиках программного и программно-аппаратного обеспечения, размещении, коммуникациях.

Поэтому для АСУ ТП основным направлением защиты является обеспечение доступности и целостности технологической информации, а обеспечение ее конфиденциальности не актуально. Однако возникает смежная угроза нарушения конфиденциальности информации «об АСУ ТП и технологическом процессе».

4. Операционный комплекс моделирования процессов нарушения информационной безопасности. Руководствуясь основными принципами и методами квалиметрии, предлагается потенциал нарушителя охарактеризовать вектором $Y^{\Pi}_{\langle 3\rangle} = Y^{\Pi}_{\langle 3\rangle}(A'_{\langle k'\rangle}; A''_{\langle k''\rangle}, B'_{\langle l'\rangle})$, $k = k' + k''$, $A_{\langle k\rangle} =< A'_{\langle k'\rangle} + A''_{\langle k''\rangle} >$ [2, 3, 4].

С позиции теории эффективности целенаправленных процессов [5] вектор $Y^{\Pi}_{\langle 3\rangle}$ есть показатель *виртуального* качества результатов ИВ. Он включает в себя три группы компонент: $Y^{\Pi}_{\langle 3\rangle} =< v, r, \tau >$, характеризующих виртуальные (возможные) целевые эффекты, где v – показатель целевых эффектов (результативность ИВ), r – показатель расходов ресурсов (ресурсоемкость ИВ), τ – затраты операционного времени (оперативность ИВ). Каждая из компонент вектора $Y^{\Pi}_{\langle 3\rangle}$ зависит от векторов $A'_{\langle k'\rangle}, A''_{\langle k''\rangle}, B'_{\langle l'\rangle}$, где $A'_{\langle k'\rangle}$ – эксплуатационно-технические характеристики (ЭТХ) и параметры системы ИВ (СиИВ) нарушителя; $A''_{\langle k''\rangle}$ – ЭТХ и параметры процесса организации ИВ (ПрИВ) или технологии ИВ; $B'_{\langle l'\rangle}$ – характеристики условий функционирования (УФС) СиИВ.

Под СиИВ будем понимать совокупность программно-аппаратных средств ИВ. Под УФС СиИВ будем понимать совокупность факторов, оказывающих влияние на параметры и ЭТХ СиИВ (вектор $A'_{\langle k' \rangle}$), а также на характеристики ПрИВ (вектор $A''_{\langle k'' \rangle}$) и через них обусловливающие возможные (виртуальные) $Y^{\Pi}_{\langle 3 \rangle}$ результаты ИВ.

Применение нарушителем средств ИВ происходит в условиях активного противодействия системы защиты атакуемой АСУ ТП. Поэтому под условиями применения $B''_{\langle l'' \rangle}$ нарушителем СиИВ будем понимать совокупность механизмов защиты атакуемой АСУ ТП. Эти защитные механизмы влияют на ситуацию, в которой СиИВ придётся выполнять задачу, и тем самым обуславливают требуемые $Y^{\partial}_{\langle 3 \rangle}(B''_{\langle l'' \rangle})$ для нарушителя результаты ИВ т.е. $Y^{\Pi}_{\langle 3 \rangle} \in \{Y^{\partial}_{\langle 3 \rangle}\}$, где $Y^{\partial}_{\langle 3 \rangle} =< v^{T}, r^{\Pi}, \tau^{Д} >$, где v^{T} – требуемый (минимально допустимый) целевой эффект v, r^{Π} – предельные (максимально допустимые) затраты ресурсов r, $\tau^{Д}$ – директивное (максимально допустимое) время τ.

Соотношение $Y^{\Pi}_{\langle 3 \rangle} \in \{Y^{\partial}_{\langle 3 \rangle}\}$ представляет собой формальное выражение цели ИВ нарушителя. Содержательно цель ИВ определяется нарушением функционирования технологических процессов, специфика защиты которых были представлены в разделе 3.

Показатель эффективности ИВ будем описывать вектором $Y^{ИВ}_{\langle 3 \rangle} = Y^{ИВ}_{\langle 3 \rangle}(A'_{\langle k' \rangle}, A''_{\langle k'' \rangle}, B'_{\langle l' \rangle}, B''_{\langle l'' \rangle})$, где $A'_{\langle k' \rangle} = A'_{\langle k' \rangle}(B'_{\langle l' \rangle}, B''_{\langle l' \rangle})$, $A''_{\langle k'' \rangle} = A''_{\langle k'' \rangle}(B'_{\langle l' \rangle}, B''_{\langle l'' \rangle})$, $B_{\langle l \rangle} =< B'_{\langle l' \rangle} + B''_{\langle l'' \rangle} >$, $l = l' + l''$.

Структурная схема операционного комплекса (ОпК) моделирования процессов нарушения ИБ изображена на рисунке 3.

Раскроем содержание основных элементов ОпК ИВ нарушителя в АСУ ТП:

- РУК – руководство нарушителя;
- ОУП – орган управления процессом ИВ;
- СиИВ – система ИВ – силы и средства ИВ;
- ПрИВ – процесс ИВ – технология (процесс организации) ИВ;
- УФС – условия функционирования СиИВ;
- УПС – условия применения нарушителем СиИВ;
- v – показатель целевых эффектов (результативность ИВ);
- r – показатель расходов ресурсов (ресурсоемкость ИВ);
- τ – затраты времени на ИВ (оперативность ИВ).

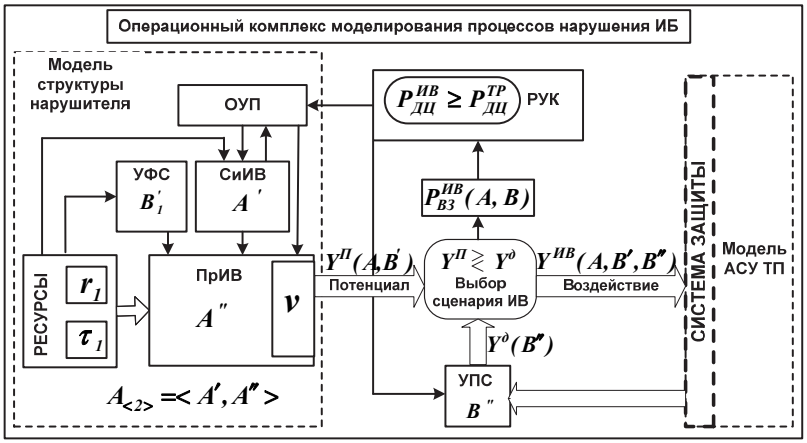

Рис. 3. Структурная схема операционного комплекса моделирования процессов нарушения ИБ

Следует понимать, что нарушитель (и реализуемые им ИВ) в инфотелекоммуникационном пространстве для защищаемой стороны представлен в виде опасных процессов – процессов нарушения ИБ. Эти деструктивные процессы совместно с процессами защиты (противодействия) образуют так называемые конфликтующие процессы, а исследование эффективности их противодействия друг другу – актуальная задача.

По сути, потенциал $Y_{\langle 3 \rangle}^{П}$ характеризует внутреннюю структуру нарушителя и может быть аналитически представлен иначе: в виде пары $< Str, Par >$, где Str – структура нарушителя, Par – значения его параметров $A'_{\langle k' \rangle}$, $A''_{\langle k'' \rangle}$, $B'_{\langle l' \rangle}$. Знание структуры Str и параметров Par позволяет классифицировать противника по различным критериям. Поэтому характеристики нарушителя будем описывать вектором $< Str, Par, Klas >$, где $Klas$ – критерий классификации нарушителя. Применяя разное сочетание параметров $A'_{\langle k' \rangle}$, $A''_{\langle k'' \rangle}$, $B'_{\langle l' \rangle}$ можно классифицировать нарушителя по множеству аспектов. Например, по параметру $A''_{\langle k'' \rangle}$ – тип реализуемого нарушителем ИВ, по параметру $B'_{\langle l' \rangle}$ – вид удаленного подключения к АСУ ТП. Поэтому в ходе аудита ИБ необходимо, прежде всего, определить класс нарушителя, а затем уже оценить его потенциал. Приведем физический смысл переменных $A'_{\langle k' \rangle}$, $A''_{\langle k'' \rangle}$, $B'_{\langle l' \rangle}$, $B''_{\langle l'' \rangle}$.

$A'_{\langle k' \rangle}$ – параметры и ЭТХ СиИВ нарушителя:

- состав и структура СиИВ;
- уровень технической компетентности нарушителя;
- характеристики средств удаленной идентификации (например, реализуемые способы сканирования удаленных хостов, настройки временных параметров сканирования; идентификации состояния TCP и UDP портов и др);
- характеристики средств ИВ (например, реализуемые классы удаленных сетевых атак и способы их реализации; возможность реализации воздействия на различных уровнях модели ISO/OSI; направленность информационного воздействия: нарушение конфиденциальности, целостности или доступности информации и др).
- характеристики системы принятия решения и др.

$A''_{\langle k'' \rangle}$ – ЭТХ и параметры ПрИВ:

- математическое описание цели ИВ;
- момент времени начала и период проведения ИВ;
- тип реализуемого ИВ;
- условие начала реализации ИВ (реализуемые по запросу от объекта атаки (ОА) или по наступлению ожидаемого события на ОА; безусловные воздействия);
- наличие обратной связи с ОА: с обратной связью; без обратной связи (однонаправленное ИВ);
- уровень эталонной модели OSI, на котором реализуется ИВ;
- сценарий проведения ИВ;
- характеристики скрытности проведения ИВ и др.

Характеристики $B'_{\langle l' \rangle}$ условий функционирования СиИВ:

- наличие точки доступа к АСУ ТП;
- вид удаленного подключения через сеть Интернет (например, коммутируемое соединение на основе PSTN; соединение с использованием ISDN; локальное соединение по технологии xDSL; использование симметричных систем спутниковой связи; использование асимметричных систем спутниковой связи; использование сотовых сетей передачи данных и др);
- уровень знаний об ОА: число и характеристики хостов; порты и сервисы, функционирующие на хостах; типы и версии операционных систем; программное обеспечение (ПО); аппаратное обеспечение; топология сети и др;
- наличие уязвимостей: уязвимости системного ПО (в том числе протоколов сетевого взаимодействия); уязвимости прикладного ПО (в том числе средств защиты информации) и др.

5. Анализ неопределенностей процесса моделировании нарушителя и оценивании эффективности его ИВ. Процесс моделирования нарушителя включает неопределенности:

Тип 1. Математической структуры нарушителя – неопределенность потенциала нарушителя – $\hat{Y}^{\,П}(\hat{A},\hat{B}')$.

Тип 2. Критерия выбора нарушителем сценария ИВ – $\hat{Y}^{\,П} \gtrless \hat{Y}^{\,д}$.

Тип 3. Показателя качества результатов ИВ – $\hat{Y}^{ИВ}_{\langle 3\rangle} = \hat{Y}^{ИВ}_{\langle 3\rangle}(\hat{A}_{\langle k\rangle}, \hat{B}_{\langle l\rangle})$.

В виду того, что как нарушителю, так и системе защите от него приходится действовать в условиях неопределенности, значения параметров векторов $\hat{A}_{\langle k\rangle}$ и $\hat{B}_{\langle l\rangle}$ оказываются случайными ($\wedge$ – символ случайной величины), а, следовательно, и вектора $\hat{Y}^{\,П}$ и $\hat{Y}^{\,ИВ}$ также будут случайными. Более того, априори случайными являются и допустимые значения $\hat{Y}^{\,д}_{\langle 3\rangle}$ вектора $\hat{Y}^{\,П}$, зависящие от системы защиты $\hat{B}''_{\langle l''\rangle}$ атакуемой АС, поскольку до проведения нарушителем ИВ сам нарушитель и поставленная им цель операции неизвестны.

Разрешение неопределенностей первого и второго типов позволяет построить модель нарушителя, а снятие неопределенностей второго и третьего типов – модель процессов нарушения информационной безопасности КИИ. На рисунке 4 приведена схематическая диаграмма, иллюстрирующая отношения перечисленных выше неопределенностей.

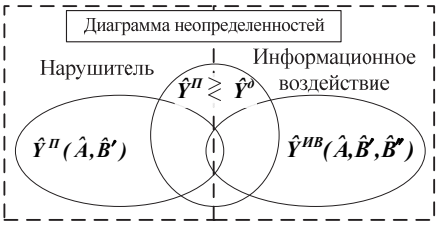

Рис. 4. Схематическая диаграмма, иллюстрирующая отношения неопределенностей процесса моделирования нарушителя и его воздействий

Рассмотрим более подробно неопределенности, с которыми приходится сталкиваться исследователю при моделировании действий нарушителя.

Во-первых, введение неопределенности в математическую структуру нарушителя, описываемую вектором $\hat{Y}^{\,П}_{\langle 3\rangle}$, позволяет отра-

зить при моделировании реальные условия неполноты сведений о нарушителе. Крайним случаем неопределенности является неструктурируемость, то есть невозможность построения соответствующей модели нарушителя, принадлежащей к тому или иному типу математической структуры. Для снятия этой "структурной" неопределенности можно предложить технологию маскирования информационных ресурсов АСУ ТП, представленной в [6]. Данная технология позволяет:

- обнаруживать скрытые каналы ИВ нарушителя на информационные ресурсы;
- формировать рефлексивное управление нарушителем с помощью обманной информационно-вычислительной среды, параметры которой описываются вектором $\hat{B}'^{*}_{\langle l' \rangle}$.

Целью маскирования является идентификация (построение модели) нарушителя, то есть определение значений параметров $\hat{A}'_{\langle k' \rangle}$, $\hat{A}''_{\langle k'' \rangle}$ и формирование вектора $\hat{Y}^{\Pi}_{\langle 3 \rangle}$. Это достигается созданием у нарушителя ложного представления об ОА путем подмены $\hat{B}'_{\langle l' \rangle}$ на $\hat{B}'^{*}_{\langle l' \rangle}$. Как следствие, реализуется возможность всестороннего исследования структуры; оценивания потенциала $\hat{Y}^{\Pi}_{\langle 3 \rangle}$; определения перечня своих защитных мер $\hat{B}''_{\langle l'' \rangle}$.

Во-вторых, существует неопределенность в задании базисных множеств и отношений, на основе которых строится модель нарушителя. Для задания количественной меры такой неопределенности можно использовать стохастический подход (стохастические структуры), базирующийся на фундаментальных положениях теории вероятностей и математической статистики, или подход с позиции теории нечетких множеств (нечеткие структуры).

Идея заключается в исследовании неопределенности выбора нарушителем того или иного сценария реализации ИВ. При данном подходе не ставится задача определения потенциала $\hat{Y}^{\Pi}_{\langle 3 \rangle}$, так как неизвестны значения параметров $\hat{A}'_{\langle k' \rangle}$, $\hat{A}''_{\langle k'' \rangle}$. Предлагается оценивать нарушителя в типах $U = \{U_i\}_{i=1}^{N}$ соответствующих возможных угроз ИВ и в "механизме выбора" $\zeta(\eta_j^i)$ сценария реализации конкретной угрозы $\eta_j^i \in U_i$. То есть в качестве модели нарушителя рассматривается его профиль $< U, \zeta >$. Перед выбором $\zeta(\eta_j^i)$ сценария нарушитель сталкивается:

- в процессе изучения специфики АСУ ТП и идентификации векторов $\hat{B}'_{\langle l' \rangle}$ и $\hat{B}''_{\langle l'' \rangle}$;

– при сравнении $\hat{Y}^{\Pi} \gtrless \hat{Y}^{o}$ и определении допустимых значений $Y^{o}_{\langle 3\rangle}(B''_{\langle l''\rangle})$ вектора $Y^{\Pi}_{\langle 3\rangle}$ своих потенциальных возможностей.

Представляется очевидным, что говорить о стохастической природе ИВ нерационально, так как нарушитель не осуществляет свой выбор случайным образом. Его выбор целенаправлен и обусловлен определенным критерием выбора.

Тогда можно говорить, что "механизм выбора" $\zeta(\eta^{i}_{j})$ характеризуется наличием тех или иных неизвестных (случайных) факторов. В этом случае необходимо ввести допущение – аудитору ИБ известно множество U типовых угроз ИБ и сценариев их реализации. Это допущение вполне обосновано, так как перечень именно типовых угроз ИБ действительно известен.

Будем различать три типа возможных ситуаций.

К *первому типу* отнесем ситуацию, когда множество угроз U и критерий выбора ζ известны. В данной ситуации профиль нарушителя известен, остается только оперативно организовать соответствующую защиту.

Второй тип включает ситуацию, при которой множество угроз U известны, а критерий выбора ζ неизвестен. В данном случае процесс управления защитой похож на процесс игры. Решением такого рода задач занимается специальный раздел математики, носящий название «Теория игр». Под теорией игр часто понимают теорию математических моделей принятия оптимальных решений в условиях неопределенности и конфликта. Однако теория игр, как математический аппарат, страдает концептуальной неполнотой. Так, в реальном конфликте перечень возможных угроз U и сценариев их реализации как раз неизвестен, и наилучшим решением для нарушителя в конфликтной ситуации нередко будет именно выйти за пределы известных сценариев ИВ.

В *третий тип* входят ситуации, когда множество угроз U, а точнее сценариев их реализации, неизвестно. В данной ситуации система защиты должна уметь оперативно пресекать неизвестные ИВ путем своевременной настройки механизмов защиты и/или контрвоздействий. Для этого система защиты должна быть наделена принципиально новым свойством, позволяющим ей оперативно предвидеть реализацию неизвестных угроз U и своевременно готовиться к ним. Такое свойство называется "*Антиципация*", которое более подробно раскрывается в [7].

В-третьих, уровень неопределенности (случайности) показателя качества результатов ИВ $\hat{Y}^{ИВ}_{\langle 3\rangle} = \hat{Y}^{ИВ}_{\langle 3\rangle}(\hat{A}_{\langle k\rangle}, \hat{B}_{\langle l\rangle})$, использующего профиль $< U, \zeta >$, характеризуется вероятностью $P^{ИВ}_{ДЦ}$ достижения цели операции и является показателем эффективности ИВ. Действительно, векторы $\hat{A}_{\langle k\rangle}$, $\hat{B}'_{\langle l'\rangle}$, а, следовательно, и $\hat{Y}^{П}_{\langle 3\rangle}$ оказываются случайными. Более того, априори случайными являются и допустимые значения $\hat{Y}^{д}_{\langle 3\rangle}$ вектора $\hat{Y}^{П}_{\langle 3\rangle}$, поскольку до проведения нарушителем ИВ нам неизвестно какими должны быть результаты этого воздействия, чтобы поставленная нарушителем цель была достигнута, т.е.

$$\begin{cases} \hat{Y}^{П}_{\langle 3\rangle} = Y^{П}_{\langle 3\rangle}\left(\hat{A}_{\langle k\rangle}, \hat{B}'_{\langle l'\rangle}\right), \\ \hat{Y}^{д}_{\langle 3\rangle} = Y^{д}_{\langle 3\rangle}\left(\hat{B}''_{\langle l''\rangle}\right). \end{cases}$$

Так как в реальных условиях критерий пригодности ИВ принимает вид $G_{Ц} : \hat{Y}^{П}_{\langle 3\rangle} \in \{\hat{Y}^{д}_{\langle 3\rangle}\}$, то $P^{ИВ}_{ДЦ} = P(\hat{Y}^{П}_{\langle 3\rangle} \in \{\hat{Y}^{д}_{\langle 3\rangle}\})$. Как видно, факт пригодности результатов операции есть случайное событие. Поэтому мера достижения нарушителем цели операции является вероятностной характеристикой. Для вычисления $P^{ИВ}_{ДЦ}$ достаточно (но не необходимо) определить благоприятные для нарушителя с профилем $< U, \zeta >$ условия реализации угроз U. Под условиями реализации ИВ понимается наличие у нарушителя информации:

- о структуре и характеристиках ИТКС;
- о наличие уязвимостей программно-аппаратного обеспечения и системы защиты.

6. Рекомендации по моделированию нарушителя ИБ. Представленные выше способы оценивания потенциала нарушителя и эффективности его воздействия носят концептуальный характер и требуют дальнейших исследований. Направление дальнейших исследований – разработка методов снятия структурной неопределенности нарушителя. Однако реализация данных подходов в рамках аудита ИБ не всегда возможна, так как требует привлечения дополнительных технических средств и времени. Поэтому в ходе проведения аудита широко используются экспертные оценки нарушителя в типах U возможных угроз ИБ, которые он способен выполнить. Соответственно, модель нарушителя должна определять предпочтения нарушителя по выбору им потенциально возможных атакующих действий – элементарных

событий нарушения ИБ, из которых формируются различные сценарии реализации угрозы ИВ. То есть перед аудитором стоит задача в обоснованном уменьшении мощности множества U. При формулировке данной задачи могут быть приняты следующие допущения о наличии данных [8]:

- уровне знаний и компетентности нарушителя;
- начальном расположении нарушителя в ИТКС, определяющем список доступных ему хостов на основе некоторой формальной модели M ИТКС;
- начальных правах нарушителя, ограничивающих множество ИВ, на основе требуемых условий для реализации ИВ.

Будем различать априорную N^A и апостериорную N^P модели нарушителя. К первому типу отнесем модель, перечень параметров и их значения которой определены без привязки к структуре исследуемой АС. Структуру ее определяют гипотезы, выдвигаемые аудиторами на основании имеющихся априорных данных и своей компетенции. В результате априорная модель нарушителя, учитывающая его предпочтения по выбору потенциально возможных атакующих действий, выглядит следующим образом:

$$N^A = < Z, H, K, G > ,$$

где Z – начальные знания нарушителя о каждом атакуемом хосте и права доступа, которыми этот нарушитель обладает; H – хосты, к которым нарушитель имеет физический или удаленный доступы до начала проведения атак; K – уровень компетентности нарушителя, т.е. классы или списки доступных ему атакующих действий, как основанных на уязвимостях, обладающих разной критичностью, так и на различных методах сбора информации; G – основные цели нарушителя, например, нарушение управляемости, наблюдаемости или идентифицируемости ТП.

Для моделирования действий нарушителя, адекватного отображения его структуры, необходимо будет разработать типовую онтологическую модель для представления знаний о нарушителях. Далее, например, в ходе проведения аудита, “насыщать” ее экспертными данными (гипотезами) о нарушителе с привязкой к конкретной АСУ ТП, тем самым формируя базу знаний BZ^N о нарушителе.

Разработка апостериорной модели нарушителя N^P заключается в нахождении соответствия q между упорядоченным множеством N^A и множеством $V^{ПАО}$ или $q = (N^A, V^{ПАО}, Q)$, где $V^{ПАО}$ – множество уязвимостей программно-аппаратного обеспечения АС. Множество

$Q \subseteq N^A \times V^{ПАО}$ определяет способ, с помощью которого осуществляется соответствие между элементами множеств N^A и $V^{ПАО}$, и, как следствие, нахождение множества уязвимостей $V^N \subseteq V^{ПАО}$, которыми может воспользоваться нарушитель N^A. Множество V^N называется областью значений соответствия q. В результате апостериорная модель нарушителя N^P принимает вид: $N^A =< Z, H, K, G, V^N >$.

Другим решением нахождения множества V^N является изменение структуры онтологической модели нарушителя с учетом сведений, полученных из базы знаний уязвимостей BZ^V.

Для количественного оценивания значения показателя потенциала нарушителя предлагается воспользоваться идеей, описанной в [9], с учетом разработанного выше ОпК (см. рис. 3). Уровень потенциала нарушителя рассматривается исключительно в контексте результатов проведенного им анализа уязвимостей и делается предположение о том, что могут ли уязвимости, идентифицированные в процессе аудита, быть использованы нарушителем с разным уровнем потенциала. При анализе потенциала ИВ, потребного нарушителю для реализации уязвимости, необходимо экспертным путем оценить значения параметров идентификации и реализации уязвимости:

- уровень технической компетентности нарушителя $(A'_{\langle k' \rangle})$;
- качество средств удаленной идентификации и ИВ $(A'_{\langle k' \rangle})$;
- затраты времени на идентификацию и реализацию уязвимости $(A''_{\langle k'' \rangle})$;
- затраты времени на непосредственный доступ к ОА при идентификации и реализации уязвимости $(A''_{\langle k'' \rangle})$;
- объем знаний об ОА $(B'_{\langle l' \rangle})$.

7. Семантические аспекты исследования процессов нарушения ИБ с позиции теории стохастической индикации. Как отмечалось выше, неопределенность показателя качества результатов ИВ $\hat{Y}^{ИВ}$ характеризуется вероятностью достижения цели операции $P_{ДЦ}^{ИВ}$, что и является показателем эффективности ИВ. Для проведения собственно оценивания эффективности $P_{ДЦ}^{ИВ}$ ИВ нарушителя требуется определить требуемое значение $P_{ДЦ}^{ТР}$ показателя эффективности ИВ $P_{ДЦ}^{ИВ}$, сформулировать и реализовать критерий пригодности $G_{ЦЭ} : P_{ДЦ}^{ИВ} \geq P_{ДЦ}^{ТР}$.

Для количественного анализа приведенной выше ситуации построим ее математическую модель. Для этого применим методы теории стохастической индикации [3, 4].

Рассмотрим дважды неопределенное высказывание в виде предиката $\hat{y} > \hat{z}$, где $\hat{z}$ и $\hat{y}$ взаимно независимые случайные переменные. Определим вероятность случайного события $\hat{A} \simeq (\hat{y} > \hat{z})$:

$$P(\hat{z} < \hat{y}) = \int_{-\infty}^{\infty} F_{\hat{z}}(y)\, dF_{\hat{y}}(y); \tag{1}$$

$$P(\hat{y} > \hat{z}) = \int_{-\infty}^{\infty} R_{\hat{y}}(z)\, dF_{\hat{z}}(z), \tag{2}$$

где $\left.\begin{array}{l} F_{\hat{x}}(x) \overset{d}{=} P(\hat{x} < x) \\ R_{\hat{x}}(x) \overset{d}{=} P(\hat{x} \geq x) \end{array}\right\}$ – функция распределения $\hat{x}$.

Введем следующие обозначения:

$$\hat{\omega}_1 = \omega_1(\hat{y}) = F_{\hat{z}}(\hat{y}); \tag{3}$$

$$\hat{\omega}_2 = \omega_2(\hat{z}) = R_{\hat{y}}(\hat{z}). \tag{4}$$

Тогда, как видно из (1) и (2), $\left.\begin{array}{l} P(\hat{z} < \hat{y}) = M[\hat{\omega}_1] = \overline{\omega}_1 \\ P(\hat{y} \geq \hat{z}) = M[\hat{\omega}_2] = \overline{\omega}_2 \end{array}\right\} \Rightarrow \overline{\omega}_1 = \overline{\omega}_2$ (5).

Случайные величины $\hat{\omega}_1$ и $\hat{\omega}_2$ называются *стохастическими супериндикаторами* [3-5]. Поскольку каждому двухместному дважды неопределенному предикату соответствуют два супериндикатора, то для отличия их друг от друга они снабжены индексами (номерами).

Из соотношения (5) следует, что:

$$P(\hat{z} < \hat{y}) = \overline{\omega}_1 = \int_0^1 \omega\, dF_{\hat{\omega}_1}(\omega) = P(\hat{y} \geq \hat{z}) = \overline{\omega}_2 = \int_0^1 \omega\, dF_{\hat{\omega}_2}(\omega),$$

где $F_{\hat{\omega}_1}(\omega)$, $F_{\hat{\omega}_2}(\omega)$ – соответственно функции распределения $\hat{\omega}_1$ и $\hat{\omega}_2$.

Супериндикаторы $\hat{\omega}_1$ и $\hat{\omega}_2$ могут принимать бесконечное множество значений из интервала $(0,1]$ и имеют смысл апостериорной вероятности высказывания A в неопределенной ситуации $\hat{\aleph}$, задаваемой $\hat{y}$ и $\hat{z}$, соответственно.

Из всего сказанного можно сделать вывод, что безусловная (априорная) вероятность случайного события $\hat{A} \simeq (\hat{z} < \hat{y})$ равна математи-

ческому ожиданию его условной (апостериорной) вероятности или, другими словами, это его средневзвешенная достоверность. При этом, достоверность события $\hat{A}$ распределена на интервале $(0,1]$ с плотностью $\varphi_{\hat{\omega}_1}(\omega)$ или $\varphi_{\hat{\omega}_2}(\omega)$. Из сказанного следует, что не только ситуация неопределенна (случайны $\hat{z}$ и $\hat{y}$), но и степень истинности соответствующего высказывания (степень достоверности события $\hat{A} \simeq (\hat{z} < \hat{y})$ случайна и может принимать значения, отличные от 0 и 1 или $\overline{\omega}_1 \neq P(\hat{\omega}_1 = 1)$; $\overline{\omega}_2 \neq P(\hat{\omega}_2 = 1)$.

Таким образом, в приведенной трактовке неопределенность ситуации $\hat{\aleph}$, в которой нарушителю придется действовать, характеризуется возможными значениями супериндикатора $\hat{\omega}$, а случайность высказывания $\hat{A}$ характеризуется вероятностью P его достоверности.

Супериндикаторы $\hat{\omega}_1$ и $\hat{\omega}_2$ совмещают в себе свойства и функции $\omega(\hat{y})$ (3) случайного аргумента и случайной функции $\hat{\omega}(y)$ (4), т.е. представляют собой случайные функции случайных аргументов.

Физический смысл таких свойств стохастических индикаторов заключается в следующем. В предикате $\hat{z} < \hat{y}$ переменная $\hat{y}$ определяет границу "*неопределенного*" ("*случайного*") множества $\hat{A} = (-\infty, \hat{y})$, при попадании в которое случайной величины $\hat{z}$ индикаторы $\hat{\omega}_1$, $\hat{\omega}_2$ могут принять уже любые значения из интервала (0, 1]. Для практического применения математического аппарата стохастических супериндикаторов необходимо знать законы их распределения. Введем обозначения:

$$\hat{\omega}_2 \overset{d}{=} R_{\hat{y}}(\hat{z}); \quad \omega = \omega(y) = R_{\hat{y}}(z); \quad z = z(\omega) = R_{\hat{y}}^{-1}(\omega).$$

Тогда, если функции распределения $R_{\hat{y}}(y)$ и $R_{\hat{z}}(z)$ случайных величин $\hat{y}$ и $\hat{z}$ известны, то:

$$F_{\hat{\omega}_2}(\omega) \overset{d}{=} P(\hat{\omega}_2 < \omega) = P\{R_{\hat{y}}(\hat{z}) < R_{\hat{y}}[z(\omega)]\} = P[\hat{z} > z(\omega)] =$$
$$= R_{\hat{z}}[z(\omega)] = R_{\hat{z}}[R_{\hat{y}}^{-1}(\omega)], \quad \omega \in (0,1].$$

В результате $F_{\hat{\omega}_2}(\omega) = R_{\hat{z}}[R_{\hat{y}}^{-1}(\omega)]$.

Как было показано выше, соотношение $Y^{\Pi}_{\langle 3\rangle} \in \{ Y^{\partial}_{\langle 3\rangle} \}$ представляет собой формальное выражение цели ИВ нарушителя. Введем следующие обозначения: $v^{T} \overset{d}{=} \hat{z}_1$; $r^{\Pi} \overset{d}{=} \hat{z}_2$; $\tau^{Д} \overset{d}{=} \hat{z}_3$.

Тогда критерий пригодности результатов ИВ, проводимого нарушителем, примет вид:

$$G_{ИР}: \ (\hat{Y}_{\langle 3\rangle} \in \{\hat{Y}^{\partial}_{\langle 3\rangle}\}) \simeq (\hat{Y}_{\langle 3\rangle} \overset{\geq}{<} \hat{Z}_{\langle 3\rangle}) \simeq [(\hat{y}_1 \geq \hat{z}_1) \cap (\hat{y}_2 \leq \hat{z}_2) \cap (\hat{y}_3 \leq \hat{z}_3)] .$$

В результате, *вероятность достижения нарушителем цели операции* будет определяться выражением:

$$P^{ИВ}_{ДЦ} = P\left(\hat{Y}_{\langle 3\rangle} \in \left\{\hat{Y}^{\partial}_{\langle 3\rangle}\right\}\right) = P\left(\hat{Y}_{\langle 3\rangle} \overset{\geq}{<} \hat{Z}_{\langle 3\rangle}\right) = \begin{cases} \int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty} \Phi_{\hat{Y}_{\langle 3\rangle}}\left(Z_{\langle 3\rangle}\right) dF_{\hat{Z}_{\langle 3\rangle}}\left(Z_{\langle 3\rangle}\right), \\ \int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty} \overline{\Phi}_{\hat{Z}_{\langle 3\rangle}}\left(Y_{\langle 3\rangle}\right) dF_{\hat{Y}_{\langle 3\rangle}}\left(Y_{\langle 3\rangle}\right). \end{cases} . \qquad (6)$$

По структуре выражений (6) видно, что $P^{ИВ}_{ДЦ}$ представляет собой математическое ожидание одной из случайных величин: $\hat{\omega}^{\langle 3\rangle}_1 \overset{d}{=} \Phi_{\hat{Y}_{\langle 3\rangle}}(\hat{Z}_{\langle 3\rangle})$ или $\hat{\omega}^{\langle 3\rangle}_2 \overset{d}{=} \overline{\Phi}_{\hat{Z}_{\langle 3\rangle}}(\hat{Y}_{\langle 3\rangle})$, называемых соответственно первым и вторым стохастическими супериндикаторами третьего ранга. Соответственно:

$$P^{ИВ}_{ДЦ} = \overline{\omega^{\langle 3\rangle}_i} = M_{\hat{\omega}^{\langle 3\rangle}_i} = M[\,\hat{\omega}^{\langle 3\rangle}_i\,] = \int\limits_0^1 \omega\, dF_{\hat{\omega}^{\langle 3\rangle}_i}(\omega) \ , \ [i = 1,2].$$

В связи с этим вероятность $P^{ИВ}_{ДЦ}$ имеет смысл средней условной (*апостериорной*) вероятности достижения цели операции.

Следует обратить внимание, что математическое ожидание $M\left[\hat{\omega}^{\langle 3\rangle}_i\right]$ случайной величины $\hat{\omega}^{\langle 3\rangle}_2$ (стохастического супериндикатора третьего ранга) дает прогноз лишь средних результатов будущих массовых опытов, тогда как закон распределения $F_{\hat{\omega}^{\langle 3\rangle}_2}(\omega)$ супериндикатора $\hat{\omega}^{\langle 3\rangle}_2$ позволяет прогнозировать результаты единичных опытов.

Если известен закон распределения $F_{\hat{\omega}^{\langle 3\rangle}_2}(\omega)$, то могут быть определены два важных показателя эффективности уникальных ИВ, называемые гарантируемыми вероятностями достижения её цели:

$$\omega^{\Gamma}_{ДЦ}(\gamma)=\begin{cases}\omega^{\Gamma}_{1}(\gamma)\overset{d}{=}R_{\hat{\omega}^{\langle 3\rangle}_{1}}(\gamma)=F_{\hat{\omega}^{\langle 3\rangle}_{1}}(1-\gamma);\\ \omega^{\Gamma}_{2}(\gamma)\overset{d}{=}R_{\hat{\omega}^{\langle 3\rangle}_{2}}(\gamma)=F_{\hat{\omega}^{\langle 3\rangle}_{2}}(1-\gamma),\end{cases}$$

где γ– уровень гарантии (*гарантийная вероятность*).

Поскольку при определении гарантируемой вероятности $\omega^{\Gamma}_{ДЦ}(\gamma)$ используется закон распределения супериндикатора $\hat{\omega}^{\langle 3\rangle}_{2}$, то этот показатель позволит оценить в будущем эффективность уникальных (единичных) операций, в отличие от вероятности $P^{ИВ}_{ДЦ}$, достаточно полно характеризующей эффективность лишь массовых операций. По своей природе реализация сценария ИВ уникальна, что говорит о большой значимости показателя $\omega^{\Gamma}_{ДЦ}(\gamma)$. Стоит отметить, что при немногократном и особенно при одноразовом применении нарушителем средства ИВ (для реализации единичного ИВ) отклонения показателя $\hat{\omega}^{\langle 3\rangle}_{2}$ эффективности ИВ от его среднего значения $\omega^{\Gamma}_{ДЦ}(\gamma)$ можетт оказаться существенным и тогда надо считаться с возможностью появления неожиданностей в каждом отдельном случае.

В определении показателя эффективности операции $\omega^{\Gamma}_{ДЦ}(\gamma)$ фигурируют две вероятности: гарантируемая – ω^{Γ} и гарантийная – γ. Для уяснения их различия дадим их частотные трактовки.

Поскольку $\omega^{\Gamma}_{ДЦ}(\gamma)$ – это наименьшее (с вероятностью γ) из значений условной вероятности $\hat{\omega}^{\langle n\rangle}=\Phi_{\hat{Y}_{\langle n\rangle}}(\hat{Z}_{\langle n\rangle})$, принимаемых ею при фиксации условий применения $B''_{\langle l''\rangle}$ нарушителем средств ИВ, т.е. при фиксации значения $\hat{Z}_{<n>}$ вектора $\hat{Z}_{\langle n\rangle}$, то $\omega^{\Gamma}_{ДЦ}(\gamma)$ имеет смысл минимально возможной (с вероятностью γ) доли реализации условий применения нарушителем средств ИВ, в которых цель операции достигается с вероятностью $\hat{\omega}^{\langle n\rangle}\geq\omega^{\Gamma}_{ДЦ}(\gamma)$. Например, следующая запись $\omega^{\Gamma}_{ДЦ}(0{,}8)=0{,}1$ соответствует $\omega^{\Gamma}_{2}(0{,}8)\overset{d}{=}R_{\hat{\omega}^{\langle 3\rangle}_{2}}(0{,}8)=P(\hat{\omega}^{\langle 3\rangle}_{2}\geq 0{,}8)=0{,}1$. Это означает, что в данный момент с вероятностью $P^{ИВ}_{ДЦ}\geq 0{,}8$ успех реализации уникального ИВ возможен только в 10% случаев.

В зависимости от динамики обстановки требования $P^{ТР}_{ДЦ}$ к показателю эффективности $P^{ИВ}_{ДЦ}$, так и сам $P^{ИВ}_{ДЦ}$ будут меняться, и как след-

ствие, они будут являться случайными величинами – $\hat{P}_{ДЦ}^{ТР}$, $\hat{P}_{ДЦ}^{ИВ}$. В результате показатель эффективности действий нарушителя принимает вид $P_{Н}^{*}(\hat{P}_{ДЦ}^{ИВ} \geq \hat{P}_{ДЦ}^{ТР})$. Эта ситуация соответствует задаче, требующей рассмотрения предиката вида $\hat{\omega}_i \geq \hat{\omega}_j$ (где $\hat{\omega}_i$, $\hat{\omega}_j$ – индексные супериндикаторы), вычисления вероятности $P(\hat{\omega}_i < \hat{\omega}_j)$ и анализа её стохастических свойств, аналогичного приведенному выше применительно к вероятности $P(\hat{y} > \hat{z})$. Для решения таких задач потребуется трансформировать распределения супериндикаторов $\hat{\omega}_i$, $\hat{\omega}_j$, которые в этом случае будут называться индикаторами *первого порядка*, в индикаторы $\hat{\omega}_{ij}^{[2]}$, $\hat{\omega}_{ji}^{[2]}$ *второго порядка* и реализовать следующую процедуру:

$$P(\hat{\omega}_j > \hat{\omega}_i) = \int_0^1 R_{\hat{\omega}_j}(\omega) dF_{\hat{\omega}_i}(\omega) = \int_0^1 \omega dF_{\hat{\omega}_{ji}^{[2]}}(\omega) = \overline{\omega_{ji}^{[2]}}.$$

8. Заключение. Процесс познания возможных нарушений ИБ бесконечен и, следовательно, на любой период времени знания исследователя содержат элемент неопределенности, а число ступеней (уровней) этого анализа может неограниченно расти. Действительно, все вероятностные модели случайных явлений строятся в предположении, что основные условия эксперимента известны. Так, в "элементарной" теории вероятностей – это комплекс $\aleph$ условий "эксперимента", в аксиоматической теории – это *пространство U элементарных событий*, в математической статистике – это *генеральная совокупность.*

Это допущение легло в основу существующих в настоящее время вероятностных моделей случайных явлений, присущих понятию ИБ. Эти модели строятся в предположении, что известны:

– условия проведения операции, например, условия проведения сценария ИВ;

– законы распределения и значения числовых характеристик исследуемых случайных величин (векторы $\hat{A}'_{\langle k' \rangle}, \hat{A}''_{\langle k'' \rangle}, \hat{B}'_{\langle l' \rangle}$).

Однако используемые в настоящее время вероятностные модели дают прогнозы лишь средних результатов будущих массовых опытов, поэтому вероятность $P_{ДЦ}^{ИВ}$ успеха ИВ, вычисленная в данных условиях, будет достаточно полно характеризовать эффективность лишь массовых воздействий, что концептуально не верно.

По своей природе реализация сценария ИВ уникальна, так как наилучшим решением для нарушителя в конфликтной ситуации будет именно выйти за пределы известных сценариев ИВ. С другой стороны,

если условия $\aleph$ проведения нарушителем ИВ (векторы $B'_{\langle l' \rangle}$, $B''_{\langle l'' \rangle}$.) до его проведения неизвестны (с достаточной полностью), то задача определения вероятностей $P_{ДЦ}^{ИВ}$ исходов ИВ становится неопределенной. Для разрешения данной проблемы – прогнозирования результатов единичных опытов, эффективен математический аппарат теории стохастической индикации. Он служит основой для разработки методов оценивания эффективности уникальных операций, для исследования которых известные вероятностные методы малопригодны.

Штатное функционирование технологического процесса зависит от качества работы множества других производственных процессов, нарушение которых является целью ИВ нарушителя. Тогда можно говорить, что выходом разработанного операционного комплекса является множество стохастических супериндикаторов, соответствующих множеству целей ИВ нарушителя. В комплексе эти супериндикаторы дают некую интегральную оценку-индикатор. Физический смысл этого индикатора характеризуется качеством системы защиты по противодействию нарушителю; относительной оценкой защищенности АСУ ТП и мерой неопределенности ситуации, в которой действует нарушитель.

Исследование в динамике значений индикатора, принимаемых им в ходе функционирования операционного комплекса, позволит в дальнейшем выявлять как сам факт присутствия нарушителя в АСУ ТП, так и доступные ему сценарии ИВ. Следует отметить прогностические возможности операционного комплекса, позволяющие исследовать нарушителя в текущий момент времени, а также генерировать с опережением новые модели нарушителя, исследовать их возможности и предлагать различные варианты защиты.

Литература

1. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). URL: http://fstec.ru (дата обращения: 27.01.2015).
2. *Горбачев И.Е., Еремеев М.А., Андрушкевич Д.В.* Методологические основы оценивания эффективности действий сторон информационного конфликта в инфотелекоммуникационных системах // Материалы 23-й научно-практической конференции “Методы и технические средства обеспечения безопасности информации”. С-Пб.: Издательство Политехнического университета. 2014. С. 11–13.
3. *Горбачев И.Е., Еремеев М.А.* К вопросу о применении стохастического супериндикатора в задачах оценивания защищенности информации в автоматизированных систем // Проблемы информационной безопасности. Компьютерные системы. 2013. № 2. С. 20–25.
4. *Горбачев И.Е., Еремеев М.А.* Подход к применению методов стохастической индикации в задачах оценивания эффективности защиты информации в автоматизированных системах // Материалы 22-й научно-практической конференции “Методы и технические средства обеспечения безопасности информации”.

СПб.: Издательство Политехнического университета. 2013. С. 14–16.
5. *Петухов Г.Б., Якунин В.И.* Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем // М.: АСТ. 2006. 504 с.
6. *Горбачев И.Е., Еремеев М.А.* Особенности технологии маскирования информационных ресурсов с применением обманных систем и управлением поведением нарушителя // Материалы 23-й научно-практической конференции “Методы и технические средства обеспечения безопасности информации”. С-Пб.: Издательство Политехнического университета. 2014. С. 13–15.
7. *Бирюков Д.Н., Ломако А.Г.* Подход к построению системы предотвращения киберугроз // Проблемы информационной безопасности. Компьютерные системы. 2013. №2. С. 13–19.
8. *Чечулин А. А.* Методика оперативного построения, модификации и анализа деревьев атак // Труды СПИИРАН. 2013. Вып. 3(26). С. 40–53.
9. ГОСТ Р ИСО/МЭК 18045-2013. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий // М.: Госстандарт России. 2014.

References

1. Oficial'nyj sajt Federal'noj sluzhby po tehnicheskomu i jeksportnomu kontrolju (FSTJeK Rossii) [Official website of the Federal Service for Technical and Export Control (FSTEC Russia)]. Available at: http://fstec.ru. (accessed 27.01.2015). (In Russ.).
2. Gorbachev I.E., Eremeev M.A., Andrushkevich D.V. [Methodological bases of evaluation of efficiency of actions of the parties to the conflict in information systems infotelecommunication]. *Materialy 23 nauchno-prakticheskoy konferenciyi “Metody I tehnicheskiye sredstva obespecheniya bezopasnosti informacii”* [Materials of the 23nd scientific and practical conference "Methods and Technical Means of Safety of Information"]. SPB: St. Petersburg Polytechnical University, 2014. pp. 11–13. (In Russ).
3. Gorbachev I.E., Eremeev M.A. [On the question of the application of stochastic superindikatora in problems of estimation of information security in automated systems]. *Problemy informatsionnoy bezopasnosty. Kompyuternie sistemy – Problems of information security. Computer systems*. SPB: St. Petersburg Polytechnical University. 2013. vol. 2. pp. 20–25. (In Russ).
4. Gorbachev I.E., Eremeev M.A. [Approach to the use of stochastic methods in problems of estimation indicating the effectiveness of the protection of information in automated systems]. *Materialy 22 nauchno-prakticheskoy konferenciyi “Metody I tehnicheskiye sredstva obespecheniya bezopasnosti informacii”* [Materials of the 22nd scientific and practical conference "Methods and Technical Means of Safety of Information"]. SPB: St. Petersburg Polytechnical University. 2013. pp. 14–16. (In Russ).
5. Petuhov G.B., Jakunin V.I. *Methodological bases of the external design of targeted processes and dedicated systems*. [Methodological bases of the external design of targeted processes and dedicated systems]. Moscow: AST. 2006. 504 p. (In Russ).
6. Gorbachev I.E., Eremeev M.A. [Features of technology of masking of information resources with use of deceptive systems and management of behavior of the malefactor]. *Materialy 23 nauchno-prakticheskoy konferenciyi “Metody I tehnicheskiye sredstva obespecheniya bezopasnosti informacii”* [Materials of the 23nd scientific and practical conference "Methods and Technical Means of Safety of Information"]. SPB: St. Petersburg Polytechnical University. 2014. pp. 13–15. (In Russ).
7. Biryukov D.N., Lomako A.G. [Approach to creation of system of cyber-threats preventing]. *Problemy informatsionnoy bezopasnosty. Kompyuternie sistemy – Problems of information security. Computer systems*. SPB: St. Petersburg Polytechnical University. 2013. vol. 2. pp. 13–19. (In Russ).
8. Chechulin A.A. [Technique of rapid construction, modification and analysis of attack

trees]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2013. vol. 3(26). pp. 40–53. (In Russ).
9. GOST R ISO/MJeK 18045-2013. [Information technology. Methods and means of ensuring safety. Methodology for Information Technology Security Evaluation]. M.: Gosstandart Rossii. 2014. (In Russ.).

Горбачев Игорь Евгеньевич — к-т техн. наук, докторант кафедры систем сбора и обработки информации, Военно-космическая академия, имени А.Ф. Можайского. Область научных интересов: исследование операций, информационная безопасность, искусственный интеллект, информационные конфликты в инфотелекоммуникационном пространстве. Число научных публикаций — 60. gie1976@mail.ru; ул. Ждановская, д. 13, 197198, Санкт-Петербург; р.т.: +7(812) 347-96-87.

Gorbachev Igor' Evgen'evich — Ph.D., doctoral student of system for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: research of operations, artificial intelligence, information security, the information conflicts in infotelekommunikatsionny space. The number of publications — 60. gie1976@mail.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 347-96-87.

Глухов Александр Петрович — к-т техн. наук, начальник департамента информационной безопасности, ОАО «РЖД». Область научных интересов: информационная безопасность, охрана объектов железнодорожного транспорта. Число научных публикаций - 40. gie76@yandex.ru; ул. Ждановская, д. 13, 197198, Санкт-Петербург; р.т.: +7(812) 347-96-87.

Gluhov Aleksandr Petrovich — Ph.D., head of department of information security, JSC «RZhD». Research interests: information security, protection of railways. The number of publications — 40. gie76@yandex.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 347-96-87.

РЕФЕРАТ

Горбачев И.Е., Глухов А.П. **Моделирование процессов нарушения информационной безопасности критической инфраструктуры.**

Нарушитель в критической инфраструктуре представлен в виде опасных процессов – процессов нарушения информационной безопасности. Эти деструктивные процессы совместно с процессами защиты образуют так называемые конфликтующие процессы, а исследование эффективности их противодействия является актуальной задачей. Существующие вероятностные модели случайных явлений в области информационной безопасности существенно ограничены и обладают концептуальными недостатками для разрешения этой задачи.

Для исследования сценариев информационных воздействий нарушителя разработан операционный комплекс моделирования процессов нарушения информационной безопасности. Одним из требованием к качеству комплекса являлось наличие у него прогностических возможностей, позволяющих генерировать с временным опережением новые модели нарушителя, исследовать их возможности, проектировать различные варианты защиты, и, как следствие, предотвращать информационные воздействия.

С этой целью обоснована математическая модель стохастического супериндикатора – агрегированного показателя качества процессов нарушения, семантический аспект которого характеризуется эффективностью противоборства конфликтующих процессов. Данный супериндикатор позволяет исследовать деструктивные процессы, характерные массовым информационным воздействиям с информативной выборкой и, как следствие, выдать прогнозы средних результатов будущих массовых опытов.

С другой стороны, рациональным решением для нарушителя в конфликтной ситуации является выход за пределы известных сценариев информационных воздействий, что говорит об их уникальности и, как следствие, их скрытности. Для исследования этих процессов известные вероятностные методы малопригодны, в то время как стохастического супериндикатор позволяет оценивать уникальные процессы и давать прогноз их развития.

Исследование в динамике значений индикаторов каждого моделируемого процесса, принимаемых ими в ходе функционирования операционного комплекса, позволит в дальнейшем выявлять факт присутствия нарушителя в критической инфраструктуре, доступные ему сценарии информационных воздействий, и как следствие, реализовать внешнее проектирование системы защиты.

SUMMARY

Gorbachev I.E., Glukhov A.P. **Modeling of Processes of Information Security Violations of Critical Infrastructure.**

Malefactor in the critical infrastructure is presented as dangerous processes - processes of information security violations. These destructive processes, together with the processes of protection form the so-called conflicting processes and study the effectiveness of their counter is an urgent task. Existing probabilistic model of random phenomena in the field of information security are severely limited and have conceptual difficulties to resolve this problem.

To investigate the effects of malefactor information scenarios the operating complex for process modeling of information security was developed. One of the requirements for the quality of the complex is the presence of a prognostic features to generate a timing advance new models malefactor explore their opportunities to design various security options, and as a result, to prevent information exposure.

The mathematical model of the stochastic super indicator – aggregate quality indicator for processes violations, semantic aspect which is characterized by the confrontation of conflicting processes, is justified. This allows to explore super indicator destructive processes of typical mass information influences with informative sample and, consequently, to give the results of future projections of average mass experiments.

On the other hand, a rational decision for the malefactor in a conflict situation is going beyond the known effects of scripting information that speaks to their uniqueness and, as a consequence, their stealth. To investigate these processes known probabilistic methods are not suitable, while stochastic super indicator allows to evaluate the unique processes and provide a forecast of their development.

Study the dynamics of the indicator values of each of the simulated process, adopted by them in the course of the operation of complex operational, will further identify the fact of the presence of the malefactor in the critical infrastructure, information available to him scenarios impacts, and as a consequence, to implement the external design of the protection system.