

Р.Р. ФАТКИЕВА
**КОМПЛЕКС МОДЕЛЕЙ ДЛЯ ОЦЕНИВАНИЯ СЕТЕВОЙ
БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ
УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ**

Фаткиева Р.Р. Комплекс моделей для оценивания сетевой безопасности автоматизированных систем управления предприятием.

Аннотация. Предприятия для управления производством и передачи данных между подразделениями используют сетевые технологии. К преимуществам этих технологий можно отнести оперативность и возможность автоматизации операционных процессов, однако в то же время увеличивается риск сетевых атак на автоматизированные системы управления. Следовательно, возникает необходимость в разработке автоматических средств мониторинга, позволяющих обнаружить несанкционированное воздействие и оперативно отреагировать на него. Система информационной безопасности предприятия должна реализовывать процессы взаимодействия компонентов и самовосстановления на протяжении всего жизненного цикла.

Предложены частные модели функционирования автоматизированных систем управления предприятием в условиях информационных угроз, учитывающие параметры состояний предприятия на разных уровнях, реализацию сетевых угроз, управляющие воздействия и так далее. Для каждой модели формируется пространство состояний предприятия и на основании проведенных испытаний определяются параметры переходов, что дает возможность представить модель в виде размеченного графа. Последовательности состояний также допускают возможность моделирования с помощью аппарата полумарковских процессов. Вероятности переходов определяются при численном решении соответствующей системы интегральных уравнений методом Лапласа – Стилтгеса.

В серии экспериментов рассмотрен процесс передачи данных как в штатном режиме функционирования, так и в условиях атаки сканирования сети. Продемонстрировано применение аппарата полумарковских процессов для выявления несанкционированной активности и создания эффективного перечня мероприятий по обеспечению безопасности. На основе вычисленных значений вероятностей переходов состояний возможно построение интегрального показателя безопасности, что способствует повышению эффективности работы предприятия.

Ключевые слова: информационная безопасность, автоматизированные системы управления, сетевые атаки, полумарковские процессы, система интегральных уравнений.

1. Введение. В условиях развития промышленного производства можно отметить основные тенденции, которые характерны для современного цикла выпуска изделия: создание инжиниринговых платформ на существующих предприятиях (использование программных решений для всех промышленных процессов); создание платформ взаимодействия для контрактных и субконтрактных производств; удаленное управление непосредственно платформами и оборудованием, построение цифровых моделей проектируемых объектов и другие тенденции. В связи с этим возникает размытие границ между информационными си-

стемами управления и оборудованием производственных комплексов, которые взаимодействуют посредством сетевых технологий. Это требует введения новых методов управления сетевой безопасностью предприятий. К частным характеристикам аппарата управления современными предприятиями можно отнести ряд специфических факторов [1]:

- наличие уровней взаимодействия для достижения целевой функции;

- наличие многослойной системы обеспечения безопасности с обратной связью;

- повсеместное использование программируемых контроллеров, которые позволяют не только дистанционно управлять киберфизическими системами, но и сформировать пространство для оперативного построения цифровых платформ с возможностью удаленного управления ими;

- возможность гибкого синтеза киберфизических систем для использования автоматизации с применением технологии обработки больших данных и аналитических методов искусственного интеллекта в процессе контроля и управления;

- изменение интерфейсов управления автоматизированных систем управления (АСУ) и автоматизированных систем управления технологическими процессами (АСУТП), которое приводит к усилению методов сбора и обработки данных о производстве, оперативном контроле и управлении, в том числе без участия человека;

- сдвиг основных ценностей от технологии производства продукции к получению информации и ее обработке, на основании которой происходит трансформация свойств проектируемых объектов для получения новых объектов с дальнейшим внедрением в производство (формирование новых моделей производства, применение «цифровых двойников»);

- использование территориально-распределенных площадок для формирования технологического цикла, в том числе с выпуском единичных заказов;

- несоответствие уровня развития научно-методического аппарата оценки и прогнозирования работы предприятия потребностям практики. В частности, на уровне физических компонентов не решены задачи количественного описания как функциональных, так и информационных показателей безопасности и методов их измерения; на уровне киберфизических компонентов не разработаны методологические основы построения системы показателей информационной безопасности, различающихся степенью детализации по представляемым уровням иерархии; на уровне интеллектуальных средств

управления не разработаны основы интеграции моделей и методов оценки статических и динамических показателей качества функционирования предприятия.

С учетом представленных характеристик структурная схема функционирования АСУ и АСУТП (рис. 1) предприятия включает в себя:

- комплекс взаимосвязанного оконечного оборудования (в том числе киберфизические системы), обеспечивающего производственный процесс;

- комплекс систем управления оконечным оборудованием (SIEM, SCADA), характеризующегося функциональной связностью;

- автоматизированные системы управления технологическим и конструкторским обеспечением производственного цикла;

- автоматизированные системы управления производством, включающие в себя системы управления функциональной и информационной безопасностью с возможностью оценки выполнения целевой функции из заданного набора целевых задач.

- информационно-телекоммуникационную среду передачи данных, обеспечивающую обмен информацией и передачу управляющих воздействий.

В связи с быстрым развитием технологий киберфизических систем и включением их в технологический цикл наблюдается отсутствие общеметодологических принципов построения единой концепции систем управления сетевой безопасностью в условиях неопределенности и нелинейности процессов, которые возникают из-за сложности и неоднозначности описания объектов, что приводит к противоречиям как в системе управления, так и в системе защиты. К видам противоречий можно отнести:

- наличие конфликтов между системами управления и средствами управления сетевой безопасностью, когда одно из средств защиты распознает другое как вторжение;

- организационно-правовые противоречия, которые возникают, когда одно правовое толкование противоречит другому. Например, несогласованность понятия «конфиденциальность информации» в Федеральном законе «Об информации, информационных технологиях и о защите информации» и понятия «конфиденциальность персональных данных» в Федеральном законе «О персональных данных»;

- экономические конфликты, когда стоимость организации защиты превышает ущерб от потери информации;

- отсутствие встроенных механизмов выявления и предупреждения конфликтов.

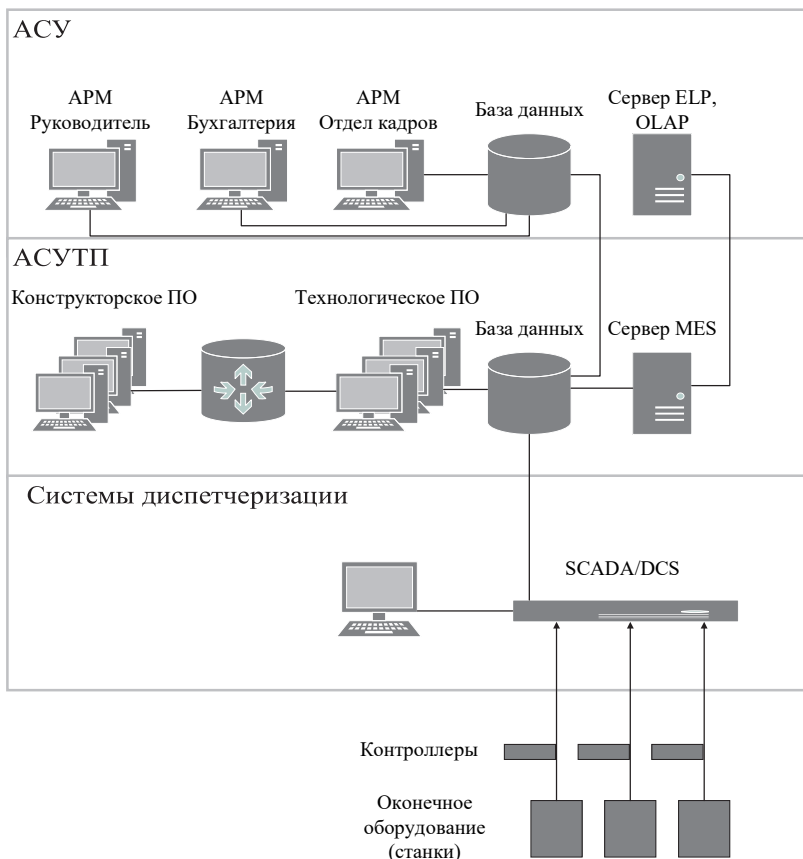


Рис. 1. Структурная схема функционирования АСУ и АСУТП

Все перечисленное приводит к необходимости внедрения систем управления информационной безопасностью предприятия. Однако до сих пор не предложена единая методология построения таких систем. Объективным препятствием к ее развитию являются противоречия между существующими теоретическими разработками, представленными научным сообществом, и отставанием внедрения технологий оперативного управления на предприятиях, в том числе и вследствие недостаточной проработки моделей сетевого взаимодействия. Не полностью проработаны модели управления АСУ и АСУТП в условиях неопределенности и вопросы обеспечения необходимой гибкости при изменении операционных циклов [2-4]. Трудность проработки систем сетевого взаимодействия связана с тем, что на сегодняшний день представлено два типа предприятий: вы-

сокотехнологичные автоматизированные линии, использующие последние разработанные технологии, и подход, основанный на совместном использовании автоматизированного и ручного труда. Интеграция и «стыковка» методов управления информационной безопасностью АСУ и АСУТП в данном случае затруднительна вследствие не только технологических разрывов обоих типов предприятий, но и существующего методологического подхода к построению производства [5, 6].

Сформированные в настоящее время методы управления сетевой безопасностью [7-9] могут быть внедрены в производственный процесс, однако такому внедрению препятствуют высокая себестоимость разработки, в частности из-за отсутствия методов формализации показателей – вследствие уникальности производственных циклов.

Еще одним противоречием является отсутствие обобщенной методологии построения единого информационного пространства сетевого взаимодействия, которое приводит к тому, что проблема не может быть решена существующими средствами. Не проработаны вопросы формализации методов обработки информации и управления, согласования политик безопасности при построении цифровой платформы, отсутствуют механизмы построения показателей безопасности по уровням интеграции в зависимости от решаемых задач.

Не проработаны вопросы взаимодействия в случае возникновения противоречий и конфликтов при выпуске изделий. Вследствие чего представленные на рынке средства обеспечения безопасности не обладают свойствами интероперабельности и масштабируемости, что приводит к возникновению проблем «стыковки» оборудования от разных производителей на разных уровнях управления, а это, в свою очередь, вызывает трудности формализации методов оценки их функционирования. Перестройка и переналадка производственных процессов требует оперативно-го изменения контура управления информационной безопасностью, что влечет за собой процесс реконфигурации показателей функционирования. Однако здесь возникают трудности сопряжения средств защиты информации, которые влекут за собой необходимость поиска комплексного многозадачного решения структурно-параметрического синтеза для обеспечения безопасного функционирования.

В этих условиях отсутствуют готовые решения, позволяющие использовать практический опыт построения инфраструктуры территориально удаленных предприятий, что приводит к недостатку доверия при создании единого информационного пространства таких предприятий при отсутствии методологического аппарата построения сетевой инфраструктуры предприятия. Отсутствие проработанной и апробированной модели доверия влечет за собой несогласованность поли-

тик безопасности, что может вызвать существенные нарушения при передаче и обработке информации.

Таким образом, при построении системы информационной безопасности предприятия необходимо учитывать возможность взаимодействия между компонентами системы безопасности, реакцию на воздействия и способность самовосстановления в случае повреждений. В целом это касается методологических подходов к защите информации на протяжении всего цикла. Однако реальное воплощение данных подходов на практике представляет определенные трудности, связанные с отсутствием единой системы показателей защищенности и получением достоверных результатов измерения [1-17]. Известные научно-методологические подходы к построению систем информационной безопасности используют мнения экспертов и упрощенные математические модели [4, 8, 10]. При огромном количестве подсистем и элементов, территориально удаленных или распределенных, задача управления требует автоматизации для быстрого реагирования на существующие угрозы. Поскольку большинство современных деструктивных воздействий проводится в автоматическом режиме, возникает необходимость разработки средств мониторинга, обработки, прогнозирования и упреждающего реагирования, позволяющих обеспечивать обнаружение несанкционированного воздействия до момента критического повреждения системы управления на любом уровне [9, 11, 13, 14]. Обнаружение аномалий процесса функционирования в результате деструктивных воздействий и борьба с ними осложняется следующими обстоятельствами: сложностью разделения информационных потоков; необходимостью обработки больших объемов данных в сжатые сроки; трудностью идентификации аномалий и местоположения источника; затруднением идентификаций уязвимостей, приводящих к реализации той или иной атаки. При этом трудности поиска местоположения, как показывает практика, возникают, даже если источник атаки находится во внутренней сети организации.

Все перечисленное требует внедрения методологического аппарата построения системы оценки безопасности типового предприятия, отражающего состояния процесса функционирования, с возможностью идентификации аномалий с учетом собранной ранее статистики.

2. Обобщенная модель функционирования предприятия.

Одним из процессов, нарушающих функционирование предприятия, являются сетевые атаки, реализуемые нарушителем через различные сети и средства связи. Современное производство позволяет обеспечить удаленный доступ к информации и оборудованию, но в то же время формирует новое пространство угроз информационной безопасности предприятия, связанное с внешним и внутренним досту-

пами к производственному процессу. Статистика сетевых атак на производственные процессы демонстрирует, что осуществление атак через компьютерные сети на АСУТП не только сохраняется на протяжении последних лет, но и имеет тенденции к росту. По данным компании «Positive Technologies» в 2019 году было зафиксировано более полутора тысяч атак, что на 19% больше, чем в 2018 году. Среди наиболее часто атакуемых объектов – различные отрасли промышленности и энергетики [18]. Увеличивается процент проникновений не только через программную часть сетевого оборудования, но и через аппаратную часть контроллеров и чипсетов. Так, в 2016 году была выявлена гигантская (почти 5 млн. устройств) ботнет-сеть, состоящая из маршрутизаторов. Проблемы с безопасностью были обнаружены в «умных» устройствах промышленных предприятий «Miele» и «AGA» [19]. Связано это и с тем, что производители устанавливают пароли на свои устройства и выпускают обновления программного обеспечения с опозданием.

Усиливается тенденция к использованию «взломанного» оборудования и программного обеспечения злоумышленниками. Имеет место проведение атаки не с целью похищения информации, а с целью воздействия на изменения технологического процесса производства. В частности, около ста компьютеров японского производителя оптического оборудования «HOYA» стали жертвами кибератаки, которая привела к частичной остановке производственных линий, поскольку они использовались для майнинга криптовалюты [20].

Продолжается рост использования загрузчиков вредоносного программного обеспечения со съемных носителей с сокрытием их в файлах с расширениями, которые включены в белые списки и потому не детектируются антивирусами, с дальнейшей загрузкой целевого вредоносного программного обеспечения из сети Интернет.

Таким образом, можно констатировать отставание разработки и внедрения средств защиты информации от интенсивного развития ИТ-технологий и технологий автоматизации производств, при которой сами средства защиты, предоставленные разными производителями, могут быть источником угрозы безопасности. Об этом свидетельствует и рост в 2019 году числа подписей вредоносного программного обеспечения с помощью легитимных сертификатов [18]. В этих условиях требуется разработать подход, позволяющий оперативно оценивать процессы функционирования предприятий и осуществлять мероприятия по защите и противодействию угрозам.

Предприятие в ходе функционирования представляет собой сложную динамическую структуру, которая может быть формализована

на в виде многоуровневых взаимосвязанных пространств состояний, элементов и протекающих процессов (рис. 1). В общем случае динамику производственной мощности можно рассмотреть как процесс изготовления единицы продукции, изменяющийся во времени вследствие улучшений, вносимых в конструкцию производимых изделий, сетевых угроз, изменений нормирования труда и так далее.

Тогда функционирование предприятия в обобщенном виде можно представить как:

$$\bar{F} = \langle \bar{X}, \bar{Y}, \bar{H}, \bar{M} \rangle,$$

где \bar{X} – вектор состояний входных воздействий; \bar{Y} – вектор состояний выходных параметров; \bar{H} – вектор внутренних состояний; \bar{M} – вектор мероприятий по обеспечению безопасности.

Анализ процесса перехода из одного заданного состояния в другое состояние под действием различных причин (внутренних, внешних, объективных, субъективных и т.п.) показывает, что, как правило, функционирование подсистем, входящих в предприятие, не изменяется непрерывно, а является постоянным на некоторых временных интервалах наблюдения $T = (t_0, t)$. Это позволяет предположить, что нештатная ситуация или сетевая атака и в самом общем случае отказ в доступе к элементу, являются возможными событиями, имеющими событийно-частотную интерпретацию, и, следовательно, могут быть обоснованно оценены и спрогнозированы в рамках статистических моделей или математических методов и моделей массового обслуживания.

3. Обобщенная модель сетевых угроз. В сложившихся условиях развития производственных процессов, при которых процесс управления осуществляется по сетевым каналам, необходимо учитывать уровни распределения передачи данных согласно взаимосвязи моделей оценки сетевых угроз (рис. 2).

Использование данного подхода позволяет отделить друг от друга внутренние процессы, протекающие в автоматизированной системе, а также осуществить контроль безопасности передачи данных на каждом из подуровней. Для управления безопасностью целесообразно ввести модели процесса функционирования операционного цикла на каждом из уровней, что позволит получить оценки, характеризующие некоторый частный срез оперативной обстановки в зависимости от поставленных задач.

В этом случае согласно рисунку 2 для правильного выбора и построения комплекса оценки сетевой безопасности целесообразно рассмотреть частные модели функционирования АСУ предприятия в условиях сетевых информационных угроз.

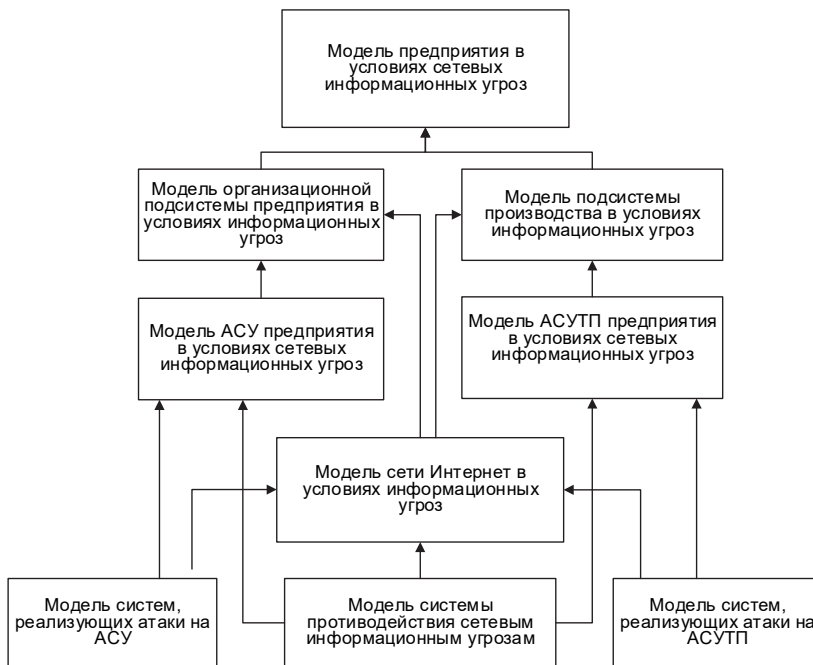
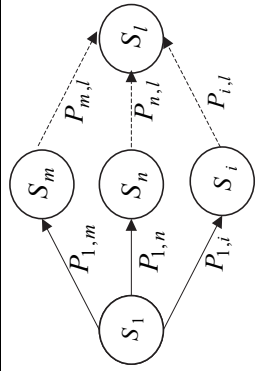
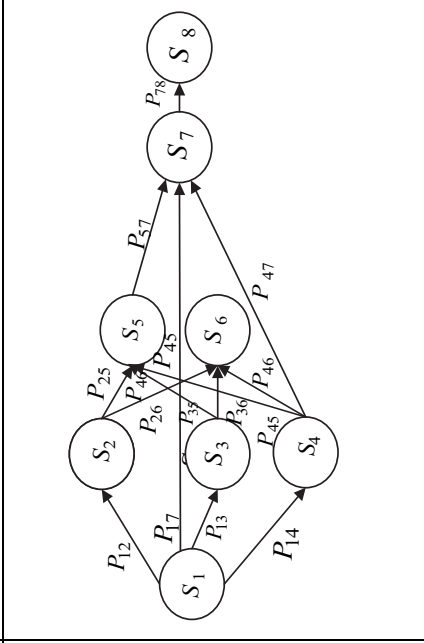


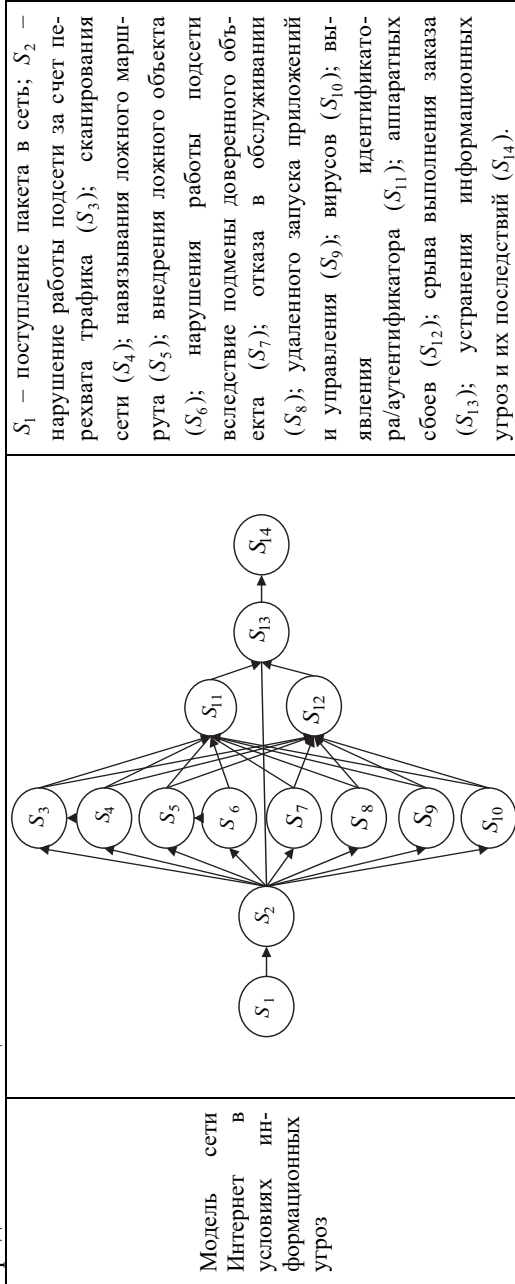
Рис. 2. Взаимосвязь моделей оценки сетевых угроз на предприятии

4. Частные модели функционирования предприятия в условиях сетевых атак. В условиях сетевых информационных угроз функционирование АСУ предприятия можно представить в виде сетевых процессов (табл. 1). Для оценки эффективности обработки информации в АСУ возможно использовать математический аппарат полумарковских процессов (ПМП), который позволяет определить зависимости перехода из одного состояния в другое от времени пребывания в заданном состоянии с учетом $\psi_i(t)$ – функции распределения времени пребывания процесса в i -х выделенных состояниях, от вероятностей p_{ij} переходов процесса из i -х состояний в j -е состояния при условии нормировки $\sum_{j=1}^N p_{ij} = 1; i = 0, 1, 2, \dots, N$ и от конечного множества состояний $\bar{S} = \langle S_1, S_2, \dots, S_N \rangle$.

Таблица 1. Система частных моделей функционирования АСУ в условиях информационных угроз

Название модели	Граф состояний	Обозначения состояний
Обобщенная модель предприятия в условиях сетевых информационных угроз	 <p>The diagram shows a state graph with nodes S_1, S_m, S_n, and S_i. Solid arrows represent transitions: $P_{1,m}$ from S_1 to S_m, $P_{1,n}$ from S_1 to S_n, and $P_{1,i}$ from S_1 to S_i. Dashed arrows represent transitions: $P_{m,i}$ from S_m to S_i, $P_{n,i}$ from S_n to S_i, and $P_{i,i}$ from S_i to S_i.</p>	<p>S_1 – поступление заказа на выпуск продукции; S_j – успешное функционирование операционного цикла; S_n – функционирование с выявлением и устранением нарушений; S_m – функционирование с угрозами, являющимися причинами отказа; S_i – завершение итерации операционного цикла.</p>
Модель организационной подсистемы предприятия в условиях информационных угроз	 <p>The diagram shows a detailed state graph with nodes S_1 through S_8. Solid arrows represent transitions with associated probabilities: P_{12} ($S_1 \rightarrow S_2$), P_{17} ($S_1 \rightarrow S_2$), P_{13} ($S_1 \rightarrow S_3$), P_{14} ($S_1 \rightarrow S_4$), P_{25} ($S_2 \rightarrow S_5$), P_{26} ($S_2 \rightarrow S_3$), P_{37} ($S_3 \rightarrow S_7$), P_{36} ($S_3 \rightarrow S_6$), P_{45} ($S_4 \rightarrow S_5$), P_{46} ($S_4 \rightarrow S_6$), P_{47} ($S_4 \rightarrow S_7$), P_{57} ($S_5 \rightarrow S_7$), P_{78} ($S_7 \rightarrow S_8$).</p>	<p>S_1 – успешное функционирование организационной подсистемы; S_2 – срыв подписания договора из-за нарушения конфиденциальности; S_3 – срыв организации тендера из-за нарушения доверия; S_4 – несоблюдение правил организации финансового учета из-за нарушения доступности и целостности; S_5 – нарушения сетевого планирования; S_6 – срыв закупки материалов; S_7 – срыв производства из-за угроз; S_8 – устранение информационных угроз и их последствий.</p>

Продолжение таблицы 1.



Продолжение таблицы 1.

<p>S_1 – получение пакета из сети; S_2 – функционирование некорректно сконфигурированного сетевого устройства; S_3 – наличие уязвимости порта; S_4 – сбор информации о подключенных устройствах; S_5 – перехват трафика; S_6 – отсутствие механизма проверки корректности заполнения заголовков служебных пакетов и данных; S_7 – отсутствие аутентификации сообщений; S_8 – отсутствие проверки корректности входных данных; S_9 – сбор информации о функционировании устройств, подключенных к сети; S_{10} – функционирование конечного устройства с неправильно сконфигурированной учетной записью; S_{11} – внедрение вредоносного ПО; S_{12} – наличие уязвимости прикладного ПО; S_{13} – наличие программной или аппаратной закладки; S_{14} – получение пакета хостом; S_{15} – получение пакета сервером; S_{16} – выполнение НСД; S_{17} – срыв выполнения заказа; S_{18} – устранение информационных угроз и их последствий</p>	<pre> graph TD S1((S1)) --> S2((S2)) S2 --> S3((S3)) S2 --> S4((S4)) S2 --> S5((S5)) S2 --> S6((S6)) S2 --> S7((S7)) S2 --> S8((S8)) S3 --> S9((S9)) S4 --> S9 S5 --> S10((S10)) S6 --> S10 S7 --> S10 S8 --> S10 S9 --> S12((S12)) S9 --> S13((S13)) S10 --> S4 S10 --> S5 S10 --> S11((S11)) S10 --> S16((S16)) S12 --> S16 S13 --> S16 S16 --> S17((S17)) S17 --> S18((S18)) </pre>
<p>Модель систем, реализующих кибератаки в АСУ</p>	

В этом случае вектор внутренних состояний \bar{H} возможно описать с использованием оценки вероятности функционирования предприятия [16-17] в штатном режиме согласно формуле:

$$P_i = \int_0^{\infty} G_{\alpha i}(t) dG_{\beta i}(t) = \int_0^{\infty} (1 - G_{\beta i}) dG_{\alpha i}(t), \quad (1)$$

где $G_{\beta i}(t)$ – функция распределения времени пребывания процесса до появления угрозы; $G_{\alpha i}(t)$ – функция распределения времени выполнения операционного цикла $t_{\alpha i}$ не превосходит с вероятностью P_i случайное время до появления угрозы $t_{\beta i}$, то есть $t_{\alpha i} \leq t_{\beta i}$.

В данной ситуации актуально определение функции распределения времени до появления нештатного входного воздействия \bar{X} , например угрозы. В работах [16, 21, 22] показано, что число событий, наступающих за промежуток времени t , распределено по закону Пуассона. Функция распределения времени пребывания ПМП в состоянии S_i определяется следующим образом:

$$F_i(t) = 1 - (1 - G_{\alpha i}(t)) \cdot (1 - G_{\beta i}(t)). \quad (2)$$

Определим вероятность перехода из состояния S_1 в состояние S_i . Переход возможен, если операционный цикл закончится раньше обнаружения угрозы, при котором $t_{\alpha i} \leq t_{\beta i}$, тогда вероятность перехода (с учетом u переменной интегрирования) определяется по следующей формуле:

$$P_{1,i}(t) = \int_0^t (1 - G_{\beta i}(u)) dG_{\alpha i}(u). \quad (3)$$

Выявление угрозы в процессе операционного цикла возможно, если $t_{\alpha i} > t_{\beta i}$. В этом случае процесс переходит из состояния S_1 в состояние S_n с необходимостью формирования мероприятий \bar{M} по восстановлению функционирования операционного цикла. Вероятность перехода в состояние S_n определяется следующим образом:

$$P_{1,n}(t) = \int_0^t (1 - G_{\alpha n}(u)) dG_{\beta n}(u). \quad (4)$$

В состоянии S_n процесс пребывает время $t_{n+1} = \min(t_{\mu n}, t_g)$, где $t_{\mu n}$ – время восстановления операционного процесса, распределенное по закону $G_{\mu n}(t)$; t_g – величина допустимого времени задержки операционного цикла, распределенная по закону $G_g(t)$. Функция распределения времени пребывания в состоянии S_n :

$$F_n(t) = 1 - (1 - G_{\mu n}(t)) \cdot (1 - G_g(t)). \quad (5)$$

Невозможность устранения угрозы в процессе функционирования операционного цикла возникает, если $t_{\alpha n} \leq t_{\beta n}$. В этом случае процесс переходит из состояния S_1 в состояние S_m , и функционирование операционного цикла полностью нарушается. Вероятность перехода в состояние S_m определяется следующим образом:

$$P_{1,m} = \int_0^t (1 - G_{\alpha m}(u)) dG_{\beta m}(u). \quad (6)$$

В состоянии S_m процесс пребывает время $t_{m+1} = \min(t_{\rho m}, t_g)$, где $t_{\rho m}$ – время функционирования операционного процесса в условиях угрозы, распределенное по закону $G_{\rho m}(t)$; t_g – величина допустимого времени задержки операционного цикла, распределенная по закону $G_g(t)$. Функция распределения времени пребывания в состоянии S_m :

$$F_m(t) = 1 - (1 - G_{\rho m}(t)) \cdot (1 - G_g(t)). \quad (7)$$

Состояние S_l определяется завершением итерации операционного цикла.

Рассмотренные вероятности перехода из состояния в состояние позволяют сформировать систему интегральных уравнений динамики

ПМП, описывающую функционирование операционного цикла в условиях угроз в виде:

$$\left\{ \begin{aligned} \psi_1(t) &= \int_0^t \psi_i(t-u)dP_{1,i}(u) + \psi_n(t-u)dP_{1,n}(u) + \psi_m(t-u)dP_{1,m}(u), \\ \psi_i(t) &= \int_0^t \psi_i(t-u)dP_{i,i}(u), \\ \psi_n(t) &= \int_0^t \psi_l(t-u)dP_{n,l}(u), \\ \psi_m(t) &= \int_0^t \psi_l(t-u)dP_{m,l}(u). \end{aligned} \right. \quad (8)$$

Решение системы уравнений (8) относительно $\psi_1(t)$ позволяет получить функцию распределения времени до появления угрозы сетевой безопасности. Система представленных интегральных уравнений решается с помощью преобразования Лапласа – Стильгеса [23].

5. Результаты моделирования системы противодействия сетевым информационным угрозам, реализующим кибератаки на АСУ предприятия. Модель передачи данных по сети в процессе функционирования предприятия с использованием сети Интернет в простейшем случае может быть представлена в виде графа (рис. 3) со следующими состояниями: 1 – получение пакета из сети; 2 – проверка IP-адреса; 3 – отбрасывание пакета; 4 – вычисление маршрута передачи данных; 5 – применение правил фильтрации трафика; 6 – обеспечение шифрования трафика; 7– обеспечение механизмов аутентификации; 8 – проверка подлинности пакета; 9 – передача на последующее устройство и/или вышестоящий уровень протокола (рис. 3).

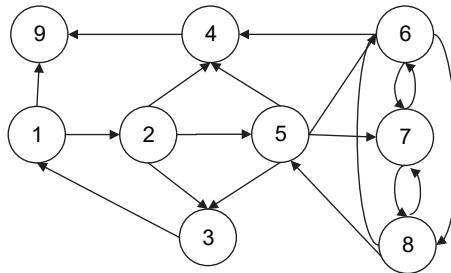


Рис. 3. Граф передачи данных в АСУ предприятия

Оценка процессов, происходящих при передаче информации, позволяет выделить четыре основных этапа, которые необходимо пройти, чтобы получить пакет конечным устройством: установление соединения и получение пакета сетевым устройством (1); проверка принадлежности полученного пакета сети и вычисление маршрута передачи данных (2-4, 9); применение правил фильтрации (5); применение механизмов защиты сетевого трафика (6, 7, 8). Каждый из этапов представляет собой последовательный набор действий, приводящий к результату, но затрудняющий работу пользователя при атаке. С другой стороны, сетевые атаки также представляют собой сложную последовательность большого числа согласованных по месту и времени этапов использования уязвимостей, приводящих к отказу работоспособности сети. Система интегральных уравнений ПМП (9), описывающая штатное функционирование сети до атаки, имеет следующий вид:

$$\left\{ \begin{array}{l} \psi_1(t) = \int_0^t \psi_2(t-u) dP_{12}(u) + \int_0^t \psi_9(t-u) dP_9(u), \\ \psi_2(t) = \int_0^t \psi_3(t-u) dP_{23}(u), \\ \psi_3(t) = \int_0^t \psi_1(t-u) dP_{31}(u), \\ \psi_4(t) = \int_0^t \psi_9(t-u) dP_{49}(u), \\ \psi_5(t) = \int_0^t \psi_3(t-u) dP_{53}(u) + \int_0^t \psi_4(t-u) dP_{54}(u) + \int_0^t \psi_6(t-u) dP_{56}(u) + \\ + \int_0^t \psi_7(t-u) dP_{57}(u) + \int_0^t \psi_8(t-u) dP_{58}(u), \\ \psi_6(t) = \int_0^t \psi_7(t-u) dP_{67}(u) + \int_0^t \psi_8(t-u) dP_{68}(u) + \int_0^t \psi_4(t-u) dP_{64}(u), \\ \psi_7(t) = \int_0^t \psi_6(t-u) dP_{76}(u) + \int_0^t \psi_8(t-u) dP_{78}(u), \\ \psi_8(t) = \int_0^t \psi_6(t-u) dP_{86}(u) + \int_0^t \psi_7(t-u) dP_{87}(u). \end{array} \right. \quad (9)$$

Решение системы интегральных уравнений относительно ψ_1 позволяет определить функцию распределения времени до наступления атаки. Вероятность безопасной передачи трафика по сети в течение времени t составляет $P = 1 - \psi_1(t)$.

Для иллюстрации оценки вероятности нарушения безопасности рассмотрим моделирование атаки сканирования сети, поскольку рассмотрение данного типа атаки позволяет получить статистические зависимости функции распределения времени появления сетевых пакетов. В связи с этим для идентификации атаки необходимо рассмотреть функционирование сети в штатном режиме (рис.3), описанное аналитически системой интегральных уравнений (9). Традиционно одним из основных этапов проникновения в сеть предприятия является этап сканирования сети и портов. Это позволяет выделить основные состояния, участвующие в формировании атаки (состояния 1-5 на рис.3).

Решение системы интегральных уравнений (9) относительно $\psi_1 - \psi_5$ (соответствующие состояниям на 1-5 рис. 3) позволяет определить вероятность передачи пакета в штатном режиме и при атаке, что дает возможность осуществить поиск вариантов управления сетевой безопасностью.

На рисунке 4 изображена вероятность передачи пакета по сети в штатном режиме функционирования (кривые соответствуют состояниям: 1 – вероятность получения пакета из сети; 2 – проверка принадлежности IP адреса; 3 – отбрасывание пакета; 4 – вычисление маршрута передачи данных; 5 – применение правил фильтрации трафика; при этом кривая 4 в явном виде на процесс развития атаки не влияет).

Вероятность сканирования сети (рис. 4б) и получение списка IP-адресов существенно не влияет на работоспособность сети и открытие соединения (кривая 1). Это может быть связано с тем, что сканирование является первым шагом в процессе развития атаки, задает ее направление и вероятный сценарий реализации. Однако, как показывает модельный пример, атаку можно обнаружить не только по количеству установленных соединений, но и по изменению количества отброшенных пакетов. Это может быть связано с возрастанием времени обработки одного пакета.

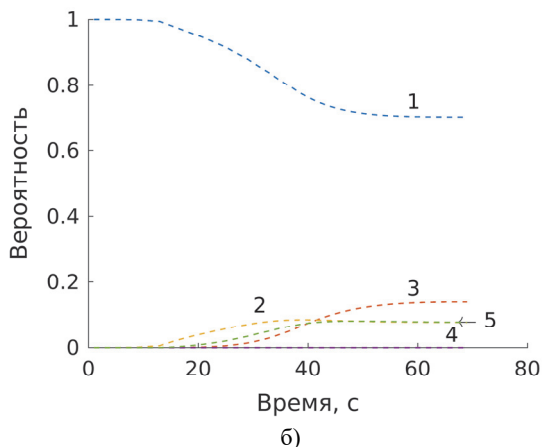
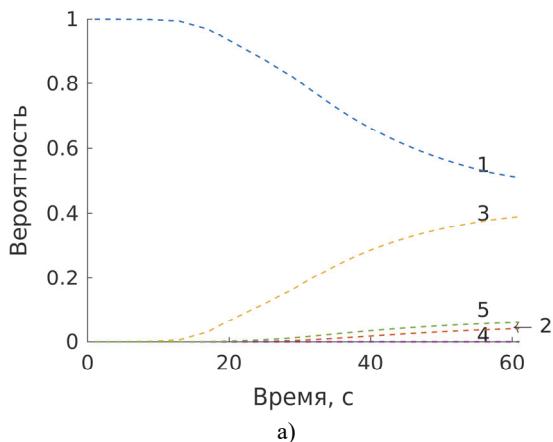


Рис. 4. Оценка вероятности передачи пакета по сети: а) в штатном режиме функционирования; б) в условиях атаки сканирования сети

Снизить вероятность процесса сканирования можно, применив настройки безопасности, например запрет на использование в сети служебных протоколов, блокировку сканирующего узла, изменение привязки порта к системным процессам, что позволяет снизить вероятность атаки без существенного прироста времени реализации цели. Полученные результаты моделирования с учетом введенных мероприятий по защите позволяют оценить влияние мер по обеспечению безопасности на уязвимые элементы в анализируемых процессах, вероятностная оценка которых представлена на рисунке 5.

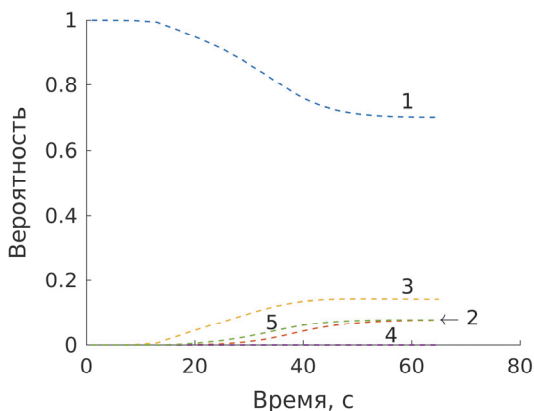


Рис. 5. Оценка вероятности получения пакета при осуществлении мероприятий по защите от сканирования сети

На рисунке 5 наблюдается картина, при которой использование комплексных средств защиты приводит к увеличению вероятности получения пакета (кривая 1) и снижению количества отбрасываемых пакетов, что может существенно уменьшить нагрузку на сеть. С другой стороны, время достижения пакетом процесса фильтрации (кривая 5) не увеличивается (по сравнению с рис. 4а), что говорит о прозрачности для пользователя введенных мер по обеспечению безопасности.

6. Заключение. Анализ составляющих процесса функционирования предприятия в плане нарастания нарушений информационной безопасности позволяет выделить классы процессов, протекающих в системе: формирование показателей функционирования предприятия; идентификацию состояний; формирование модели нарушителя; поиск вариантов управления, обеспечивающих максимальную близость к целевому состоянию; адаптацию модели управления при изменении условий функционирования или получении новой апостериорной информации о внешних воздействиях. В этих условиях возникает необходимость разработки подхода, позволяющего оперативно оценивать процессы функционирования предприятия и осуществлять мероприятия по защите от угроз и противодействию атакам. Для правильного выбора и построения комплекса средств обеспечения безопасности целесообразно рассмотреть частные модели функционирования АСУ предприятия в условиях сетевых информационных угроз. На примере задачи обнаружения сетевой активности (атак сканирования сети) продемонстрировано использование полумарковской модели для выявления атаки и формирования мероприятий по обеспечению безопасности. Аналогичная мето-

дика может быть использована для представленных частных моделей. Применение полученных результатов в процессе построения, эксплуатации и модернизации системы информационной безопасности предприятия ведет к повышению эффективности получения пакета согласно графикам (рис. 4 и 5) на 20% и дает возможность оперативно управлять процессом информационной безопасности.

Дальнейшие исследования целесообразно осуществлять в направлении поиска совокупности моделей и методов многокритериального планирования структурно-функционального синтеза средств защиты информации, позволяющих повысить эффективность функционирования промышленных объектов, сократить временные и финансовые издержки при нарушении безопасности за счет быстрого и высококачественного моделирования сценариев взаимодействия систем, которые составляют промышленный объект, для развития методов мониторинга и прогнозирования на основе их формализованного описания.

Литература

1. *Зегжда Д.П. и др.* Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасности. 2018. №2 (26). С. 2–15.
2. *Касаткина Т.И. и др.* Математическое моделирование процесса оценки безопасности обработки информации в автоматизированной системе управления // Промышленные АСУ и контроллеры. 2017. № 1. С. 15–28.
3. *Wang Y., Anokhin O., Anderla R.* Concept and use Case Driven Approach for Mapping IT Security Requirements on System Assets and Processes in Industrie 4.0 // System. 2017. vol. 1. pp. 207–212.
4. *Шнурков П.В., Горюенин А.К., Белоусов В.В.* Аналитическое решение задачи оптимального управления полумарковским процессом с конечным множеством состояний // Информатика и ее применения. 2016. Т. 10. № 4. С. 72–88.
5. *Енина Е.П.* Оценка показателей результативности процессов функционирования на предприятиях машиностроения // Вестник Воронежского государственного технического университета. 2016. Т. 12. № 6. С. 126–130.
6. *Васильев В.И., Гвоздев В.Е., Гузаиров М.Б., Кириллова А.Д.* Система поддержки принятия решений по обеспечению информационной безопасности автоматизированной системы управления технологическими процессами // Информация и безопасность. 2017. Т. 20. № 4. С. 618–623.
7. *Timpson D., Moradian E.* A Methodology to Enhance Industrial Control System Security // Procedia Computer Science. 2018. vol. 126. pp. 2117–2126.
8. *Koelemeijer D.* Enhancing the Cyber Resilience of Critical Infrastructures through an Evaluation Methodology Based on Assurance Cases // Procedia Computer Science. 2018. vol. 126. pp. 1779–1791.
9. *Fatkieva R.R.* Systems of Information Security Indicators for Industrial Enterprises // Automatic Documentation and Mathematical Linguistics. 2019. vol. 53. no. 4. pp. 216–224.
10. *Xu W., Tao Y., Yang C., Chen H.* MSICST: Multiple-Scenario Industrial Control System Testbed for Security Research // CMC-Computers, Materials & Continua. 2019. vol. 60(2). pp. 691–705.

11. *Bakker O.J. et al.* Toward Process Control from Formal Models of Transformable Manufacturing Systems // *Procedia CIRP*. vol. 63. 2017. pp 521–526.
12. *Фаткиева Р.Р.* Моделирование автоматизированных технологических процессов в условиях информационных угроз // *Научный вестник НГТУ*. 2018. № 1(70). С. 167–176.
13. *Arpishkin M.I., Vulfin A.M., Vasilyev V.I., Nikonov A.V.* Intelligent integrity monitoring system for technological process data // *Journal of Physics: Conference Series*. 2019. vol. 1368(5). pp. 052029.
14. *Sun W. et al.* A Novel Device Identification Method Based on Passive Measurement // *Security and Communication Networks*. 2019. vol. 2019. 11 p.
15. *Jiang B., Zhu X., Huang D., Braatz R.D.* Canonical variate analysis-based monitoring of process correlation structure using causal feature representation // *Journal of Process Control*. 2015. vol. 32. pp. 109–116.
16. *Лезков К.Е.* Модели и методы мониторинга параметров, характеризующих состояние инфокоммуникационной системы специального назначения // *T-Comm*. 2016. Т. 10. № 1. С. 11–17.
17. *Новиков И.С.* Методы расчёта количественных показателей надёжности сложных программных комплексов на стадии проектирования и разработки // *Труды СПИИРАН*. 2008. Вып. 6. С. 86–111.
18. Официальный сайт компании «Positive Technologies». Актуальные киберугрозы: итоги 2019 года. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019/> (дата обращения: 17.04.2020).
19. *Кусков В.* Умные и уязвимые: опасности IoT-устройств // *Информационная безопасность*. 2017. № 5. С. 22–23.
20. Ландшафт угроз для систем промышленной автоматизации. Первое полугодие 2019. URL: https://ics-cert.kaspersky.ru/media/H1_2019_kaspersky_ICS_REPORT_RUS.pdf (дата обращения: 27.04.2020).
21. *Сидорова О.И.* Пуассоновская модель трафика с бесконечным числом неоднородных источников // *Вестник ТвГУ. Серия: Прикладная математика*. 2015. № 1. С. 47–66.
22. *Черниговский А.В., Кривов М.В.* Основные модели сетевого трафика // *Вестник Ангарского государственного технического университета*. 2017. № 11. С. 137–143.
23. *Броди С.М., Власенко О.Н., Марченко Б.Г.* Расчёт и планирование испытаний систем на надёжность // *Наукова думка*. 1970. 192 с.

Фаткиева Роза Равильевна — канд. техн. наук, доцент, старший научный сотрудник, лаборатория информационно-вычислительных систем и технологии программирования, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: информационная безопасность, моделирование информационных систем. Число научных публикаций — 50. rikki2@yandex.ru; 14-я линия В.О., 39, 199178, Санкт-Петербург, Россия; р.т.: +7(812)328-4369; факс: +7(812)328-4450.

R. FATKIEVA

**COMPLEX OF MODELS FOR NETWORK SECURITY ASSESSMENT
OF INDUSTRIAL AUTOMATED CONTROL SYSTEMS**

Fatkieva R. Complex of Models for Network Security Assessment of Industrial Automated Control Systems.

Abstract. The modern enterprises apply network technologies to their automated industrial control systems. Along with advantages of the above approach the risk of network attacks on automated control systems increases significantly. Hence there is an urgent need to develop automated monitoring means being capable of unauthorized access detection and of an adequate response to it. The enterprise security system should take into account components interaction and involve the ability of self-renewal throughout the entire life cycle.

The partial models of functioning of automated control systems of an enterprise under information threats are offered taking into account parameters of states of the enterprise at its different levels, realization of network threats, counteraction measures, etc. For each model it is possible to form the state space of a part of an enterprise and on the basis of the series of tests to define state transition parameters thus enabling model representation in the form of a marked graph. The sequences of states possess the properties of semi-Markov processes so semi-Markov apparatus is applicable. Probabilities of state transitions could be computed as a result of numerical solution of the corresponding system of integral equations by Lagrange-Stieltjes technique.

Application of Semi-Markov apparatus for the detection of non-authorized activities during data transfer under network scanning attack proved the validity of the above methods. In their application results in creation of a set of security assurance measures to be undertaken. Having obtained state transition probabilities the development of integral security indicator becomes possible thus contributing to the enterprise performance enhancement.

Keywords: Information Security, Automated Control Systems, Network Attacks, Semi-Markov Processes, Integral Equations System.

Fatkieva Roza — Ph.D., Associate Professor, Senior Researcher, Laboratory of Computing and Information Systems and Programming Technologies, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: information security, modeling of information systems. The number of publications — 50. rikki2@yandex.ru; 39, 14-th Line V.O., 199178, St. Petersburg, Russia; office phone: +7(812)328-4369; fax: +7(812)328-4450.

References

1. Zegzhda, D. [Cybersecurity advanced production technologies in the era of digital transformation]. *Voprosy Kiberbezopasnosti – Issues of Cybersecurity*. 2018. vol. 2(26). pp. 2–15. (In Russ.).
2. Kasatkina T.I. et al. [Mathematical Modeling of Process Security Assessment Information Processing in Automated Control System]. *Promyshlennyye ASU i kontrolyery – Industrial Automatic Control Systems and Controllers*. 2017. vol. 1. pp. 15-28. (In Russ.).
3. Wang Y., Anokhin O., Anderla R. Concept and use Case Driven Approach for Mapping IT Security Requirements on System Assets and Processes in Industrie 4.0. *System*. 2017. vol. 1. pp. 207–212.
4. Shnurkov P.V., Gorshenin A.K., Belousov V.V. [Analytical solution of the optimal control task of a semi-Markov process with finite set of state]. *Informatika i eyo Primeneniya – Informatics and Applications*. 2016. Issue 10. vol. 4. pp. 72–88. (In Russ.).
5. Enina E.P. [The Assessment of the Efficiency of the Processes Functioning at Machine-building Enterprises]. *Vestnik Voronezhskogo gosudarstvennogo tekhnich-*

- eskogo universiteta – Bulletin of Voronezh State Technical University*. 2016. Issue 12. vol. 6. pp. 126–130. (In Russ.).
6. Vasiliev V.I., Gvozdev V.E., Guzairov M.B., Kirillova A.D. [Decision Support System for ensuring information security of automated technological processes control system]. *Informasiya i Besopasnost' – Information and Security*. 2017. Issue. 20. vol. 4. pp. 618–623. (In Russ.).
 7. Timpson D., Moradian E. A Methodology to Enhance Industrial Control System Security. *Procedia Computer Science*. 2018. vol. 126. pp. 2117–2126.
 8. Koelemeijer D. Enhancing the Cyber Resilience of Critical Infrastructures through an Evaluation Methodology Based on Assurance Cases. *Procedia Computer Science*. 2018. vol. 126. pp. 1779–1791.
 9. Fatkueva R.R. Systems of Information Security Indicators for Industrial Enterprises. Automatic Documentation and Mathematical Linguistics. 2019. vol. 53. no. 4. pp. 216–224.
 10. Xu W., Tao Y., Yang C., Chen H. MSICST: Multiple-Scenario Industrial Control System Testbed for Security Research. *CMC-Computers, Materials & Continua*. 2019. vol. 60(2). pp. 691–705.
 11. Bakker O.J. et al. Toward Process Control from Formal Models of Transformable Manufacturing Systems. *Procedia CIRP*. vol. 63. 2017. pp 521–526.
 12. Fatkueva R.R. [Modeling automated technological processes under conditions of information threats]. *Nauchnyi vestnik Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Science bulletin of the Novosibirsk state technical university*. 2018. vol. 1 (70). pp. 167–176. (In Russ.).
 13. Arpishkin M.I., Vulfina A.M., Vasilyev V.I., Nikonov A.V. Intelligent integrity monitoring system for technological process data. *Journal of Physics: Conference Series*. 2019. vol. 1368(5). pp. 052029.
 14. Sun W. et al. A Novel Device Identification Method Based on Passive Measurement. *Security and Communication Networks*. 2019. vol. 2019. 11 p.
 15. Jiang B., Zhu X., Huang D., Braatz R.D. Canonical variate analysis-based monitoring of process correlation structure using causal feature representation. *Journal of Process Control*. 2015. vol. 32. pp. 109–116.
 16. Legkov K.E. [Models and Methods of Monitoring Parameters Characterizing the State of the Infocommunication Systems of a Special Purpose]. *T-Comm – Journal T-Comm*. 2016. Issue 10. vol. 1. pp. 11–17. (In Russ.).
 17. Novikov I.S. [Calculation Methods for Quantitative Indicators of Complex Software System Reliability at the Design and Development Stages]. *Trudy SPIIRAS – SPIIRAS Proceedings*. 2008. vol. 6. pp. 86–111 (In Russ.).
 18. Oficial'nyj sajt kompanii «Positive Technologies». Aktual'nye kiberugrozy: itogi 2019 goda. [Official website of the company "Positive Technologies". Current cyber threats: results of 2019] Available at: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019> (accessed: 17.04.2020).
 19. Kuskov V. [Smart and vulnerable: the dangers of IoT devices]. *Informacionnaya bezopasnost' – Information security*. 2017. vol. 5. pp. 22–23. (In Russ.).
 20. Landshaft ugroz dlya sistem promyshlennoj avtomatizacii. Pervoe polugodie 2019. [Landscape of threats to industrial automation systems. First six months of 2019]. Available at: https://ics-cert.kaspersky.ru/media/H1_2019_kaspersky_ICS_REPORT_RUS.pdf (accessed: 27.05.2020).
 21. Sidorova O.I. [On infinite source Poisson model with heterogeneous sources]. *Vestnik TvGU. Seriya: Prikladnaya matematika – Bulletin of Tver State University. Series: Applied Mathematics*. 2015. vol. 1. pp. 47–66. (In Russ.).
 22. Chernigovskiy A.V., Krivov M.V. Models of Network Traffic]. *Vestnik AnGT – Bulletin of the Angara state Technical University*. 2017. vol. 11. pp. 137–143. (In Russ.).
 23. Brody S.M., Vlasenko O.N., Marchenko B.G. *Raschyot i planirovanie ispytaniy sistem na nadyozhnost'* [Calculation and planning of reliability tests of systems]. *Naukova dumka*. 1970. 192 p. (In Russ.).