УДК 004.056

АБСТРАКТНАЯ И ФОРМАЛЬНАЯ МОДЕЛИ БЕЗОПАСНОСТИ ПРИ ИНФОРМАЦИОННО-ТЕХНИЧЕСКОМ ВЗАИМОДЕЙСТВИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

И.В. Левчунец.
Главное управление «Национальный центр управления в кризисных ситуациях МЧС России».
А.В. Максимов, кандидат технических наук;
А.Н. Метельков, кандидат юридических наук.
Санкт-Петербургский университет ГПС МЧС России

Рассматриваются модели безопасности при организации информационно-технического взаимодействия гетерогенных автоматизированных информационных систем в связи с созданием в России единого информационного пространства в цифровой экономике и государственном управлении. Выявляются основные, значимые с точки зрения информационной безопасности, элементы автоматизированных систем. Описывается механизм возникновения потенциальных новых уязвимостей. Предлагается подход для их выявления на основе анализа приведенных моделей в сочетании с последующим использованием метода экспертных оценок, выделение вновь появляющихся в процессе интеграции автоматизированных информационных систем актуальных угроз и проведение их анализа с учетом оценки совокупного уровня опасности совместной эксплуатации уже существующих в каждой из систем и вновь возникших в процессе интеграции уязвимостей.

Ключевые слова: безопасность при интеграции систем, безопасное информационно-техническое взаимодействие, модель безопасности при интеграции

ABSTRACT AND FORMAL SECURITY MODELS IN INFORMATION AND TECHNICAL INTERACTION OF AUTOMATED SYSTEMS

I.V. Levchunets. Headquarters «National crisis management centre of EMERCOM of Russia».
A.V. Maximov; A.N. Metelkov.
Saint-Petersburg university of State fire service of EMERCOM of Russia

Security models are considered in the organization of information and technical interaction of heterogeneous automated information systems in connection with the creation of a unified information space in the digital economy and public administration in Russia. The main elements of automated systems that are significant from the point of view of information security are identified. The mechanism of potential new vulnerabilities is described. An approach is proposed for their identification based on the analysis of the given models in combination with the subsequent use of the expert evaluation method. We propose an approach based on the creation of models in combination with the subsequent use of expert evaluation method highlighting emerging in the process of integrating automated information systems relevant threats and their analysis based on an assessment of the cumulative danger level joint operation existing in each system and re-emerged in the process of integration of vulnerability.

Keywords: security during the integration of systems, secure information and technical interaction, security model for integration

Бурное развитие и повсеместное внедрение различных информационных систем практически во все сферы деятельности современного информационного общества, а также

заданный на государственном уровне курс на цифровизацию всех основных сфер жизнедеятельности людей привели, с одной стороны, к необходимости автоматизации и оптимизации ряда информационных процессов, а, с другой – к реализации и дальнейшему совершенствованию информационно-технического взаимодействия (ИТВ) функционирующих, а также вновь разрабатываемых и внедряемых информационных систем. В процессе интеграции возникает ряд проблем, связанных, в том числе с реализацией политики безопасности гетерогенных информационных систем (аппаратная и программная совместимость, согласование языков и форматов сообщений, вопросы резервирования, аттестации, сертификации, лицензирования, учет и соблюдение различных степеней секретности и уровней конфиденциальности обрабатываемой информации и т.п.).

При этом обеспечение информационной безопасности в процессе реализации интеграционных механизмов и при дальнейшей эксплуатации информационных систем нередко совсем упускаются из виду, либо реализуется формально.

Под интеграцией автоматизированных информационных систем в широком смысле в рамках данной статьи будем понимать любое ИТВ таких систем.

Как известно, в нормативных правовых актах и научной технической литературе существует целый ряд точек зрения на содержание понятий «информационная система», «автоматизированная система» и их классификацию, ведутся нескончаемые дискуссии. В Информационном сообщении Федеральной службы по техническому и экспортному контролю (ФСТЭК) России от 15 июля 2013 г. № 240/22/2637 даны разъяснения по вопросу применения рассматриваемых понятий. В частности, в Требованиях, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17, и Составе и содержании мер, утвержденных приказом ФСТЭК России от 18 февраля 2013 г. № 21, используется понятие «информационная система», установленное Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». При этом понятие «государственная информационная система», цели и порядок ее создания, а также порядок эксплуатации установлены ст.ст. 13 и 14 указанного федерального закона. В иных методических документах и национальных стандартах в области защиты информации используется понятие «автоматизированная система», определенное национальным стандартом ГОСТ 34.003–90. Учитывая, что Требования и Состав и содержание мер разрабатывались во исполнение федеральных законов от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 27 июля 2006 г. № 152-ФЗ «О персональных данных», соответственно, в которых используется понятие «информационная система», в нормативных правовых актах ФСТЭК России также используется указанное понятие.

Исходя из родственных определений понятия «информационная система», установленного Федеральным законом от 27 июля 2006 г. № 149-ФЗ, и понятия «автоматизированная система», установленного Национальным стандартом ГОСТ 34.003–90, а также из содержания Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17, и Состава и содержания мер, утвержденных приказом ФСТЭК России от 18 февраля 2013 г. № 21, использование в нормативных правовых актах ФСТЭК России понятия «информационная система» не влияет на конечную цель защиты информации и, следовательно, на построение математической модели с использованием теории графов. Авторы, разделяя в целом такой подход, используют в статье понятие «автоматизированная информационная система».

Компонентом автоматизированной информационной системы будем считать элемент одного из основных видов обеспечения (технического, программного, информационного и др.), выполняющий определённую функцию в подсистеме автоматизированной информационной системы и обеспечивающий её работу.

При декомпозиции ИТВ двух автоматизированных информационных систем можно выделить следующие основные виды обеспечения, характерные для автоматизированных систем любого типа: техническое (телекоммуникационное оборудование – ТКО, серверы,

непосредственно автоматизированные рабочие места (АРМ), информационное (информационные ресурсы) и программное обеспечение, а также ИТ-сервисы.

При этом, независимо от степени интеграции автоматизированных информационных систем и используемого способа организации ИТВ, помимо уже существующих интегрируемых систем следует отметить необходимость создания компонентов взаимодействия, реализующих и обеспечивающих определенный механизм интеграции.

С целью выявления особенностей, влияющих на информационную безопасность сопряжения информационных систем, целесообразно выделить и учесть некоторые аспекты организации такого взаимодействия:

– существование множества угроз информационной безопасности и уязвимостей отдельных компонентов [1];

– содержание различной информации ограниченного доступа (особо следует отметить возможность обработки информации, содержащей сведения, составляющие государственную тайну, различных степеней секретности) во взаимодействующих информационных системах;

– наличие потенциальных внутренних (так называемых «инсайдерских») угроз со стороны пользователей, операторов, администраторов и т.п.;

– реализация различных ИТ-сервисов, обеспечивающих работу пользователей в каждой из систем, самих систем и информационный обмен между ними [2];

– возможное присутствие разнородного аппаратного и программного (в том числе системного) обеспечения как внутри каждой из систем, так и в реализации механизма взаимодействия;

– в зависимости от масштаба распределённых систем и других факторов может иметь место территориальная удаленность компонентов каждой из систем и самих информационных систем.

Для формирования модели угроз при ИТВ предлагается учитывать взаимодействие активов информационных систем схематически представленное на рис. 1.

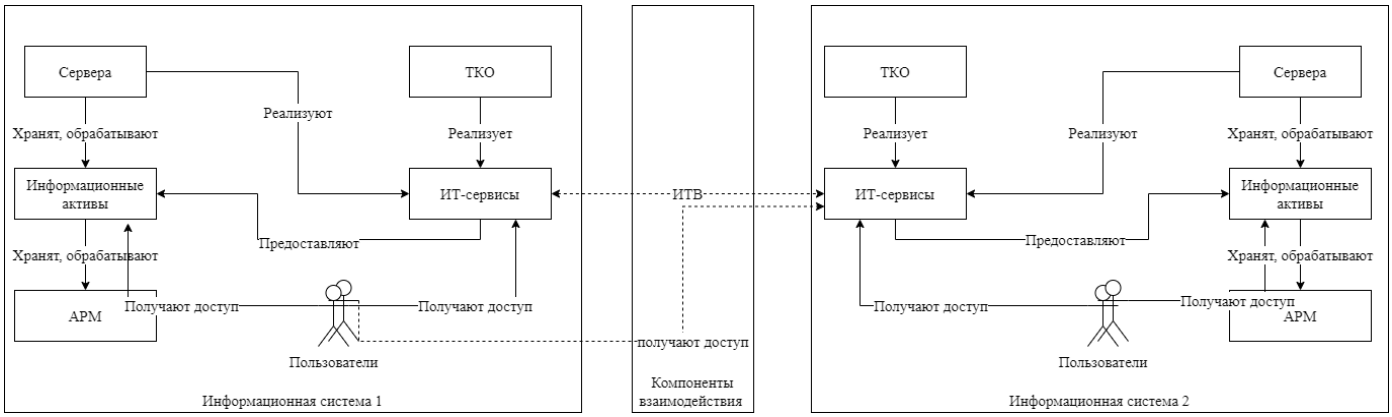

Рис. 1. **Схема взаимодействия активов информационных систем при ИТВ**

Для описания информационных процессов с точки зрения информационной безопасности традиционно принято использовать модель системы защиты с полным перекрытием [3], учитывающую следующие основные компоненты: «множество активов», «множество угроз» и «множество мер защиты», формирующих соответствующие механизмы безопасности.

Введём следующие обозначения: $A=\{a_j\}$ – множество активов защищаемой системы; $V=\{v_m\}$ – множество уязвимостей; $S=\{s_l\}$ – множество источников угроз, которые совместно формируют $T=\{t_i\}$ – множество угроз; $U=\{u_k\}$ – множество мер безопасности.

В случае представления всех отношений вида «угроза (T) ⇔ актив (A)» с применением двухдольного графа, механизм защиты фактически сводится к модели,

предполагающей перекрытие всех возможных рёбер этого графа путем использования элементов множества U (меры безопасности). Таким образом, для каждого отношения должно существовать не менее одной меры безопасности, защищающей актив a_j от реализации угрозы t_i.

Следует учитывать, что при реализации системы защиты информации в каждой из информационных систем в отдельности, когда приняты все защитные меры, и, следовательно, все рёбра графа перекрыты, процесс интеграции двух самостоятельных защищенных систем может привести к следующим ситуациям (в том числе симметричным для каждой из систем):

– для одной или более уязвимостей системы 1 существует не менее одного источника угроз в системе 2;

– для одной или более уязвимостей системы 1 существует не менее одного источника угрозы в компонентах взаимодействия;

– для одной или более уязвимостей в компонентах взаимодействия существует источник угрозы в системе 1;

– угрозы с учетом уязвимости формируются непосредственно в компоненте взаимодействия.

Для каждой из вновь возникающих угроз можно указать не менее одного свойства информации, на которые она потенциально может повлиять:

– целостность, заключающуюся в том, что данные не изменяются или не уничтожаются недозволенным способом;

– конфиденциальность, то есть предотвращение раскрытия информации перед посторонними лицами без разрешения ее владельца;

– доступность, то есть состояние, при котором субъекты с соответствующими правами доступа к защищаемой информации смогут беспрепятственно их реализовать.

Схематическое взаимодействие рассмотренных элементов каждой из автоматизированных систем при интеграции представлено на рис. 2 (двойной линией обозначены примеры угроз, возникающих при интеграции).

Таким образом, в процессе интеграции автоматизированных систем существует возможность появления дополнительных элементов, которые не были учтены в модели безопасности каждой из систем. В ситуациях, когда существует организационная и техническая возможность выявления и полного анализа указанных элементов модели безопасности и их взаимодействия между собой, при выборе мер защиты информации следует по аналогии механизму перекрытия, описанному выше, обеспечить реализацию защитных мер для вновь выявленных множеств уязвимостей и активов.

Однако в ряде случаев возможно внесение некоторой неопределенности в части возможного влияния вновь выявленных угроз информационной безопасности на активы каждой из систем, вследствие чего может быть затруднена реализация «общей» модели безопасности для интегрируемых систем. Более того, в ситуациях, связанных с техническими и организационными ограничениями при создании системы защиты информации в одной из систем, может быть недоступна исчерпывающая информация как об источниках угроз другой системы, так и о некоторых элементах механизма интеграции.

Отдельно следует упомянуть, что вновь выявленные угрозы и уязвимости могут при взаимодействии с уже существующими и нейтрализованными (при проведении мероприятий по защите информации в каждой из автоматизированных систем) угрозами сформировать дополнительные уязвимости следующего порядка (взаимодействие уязвимостей) [4].

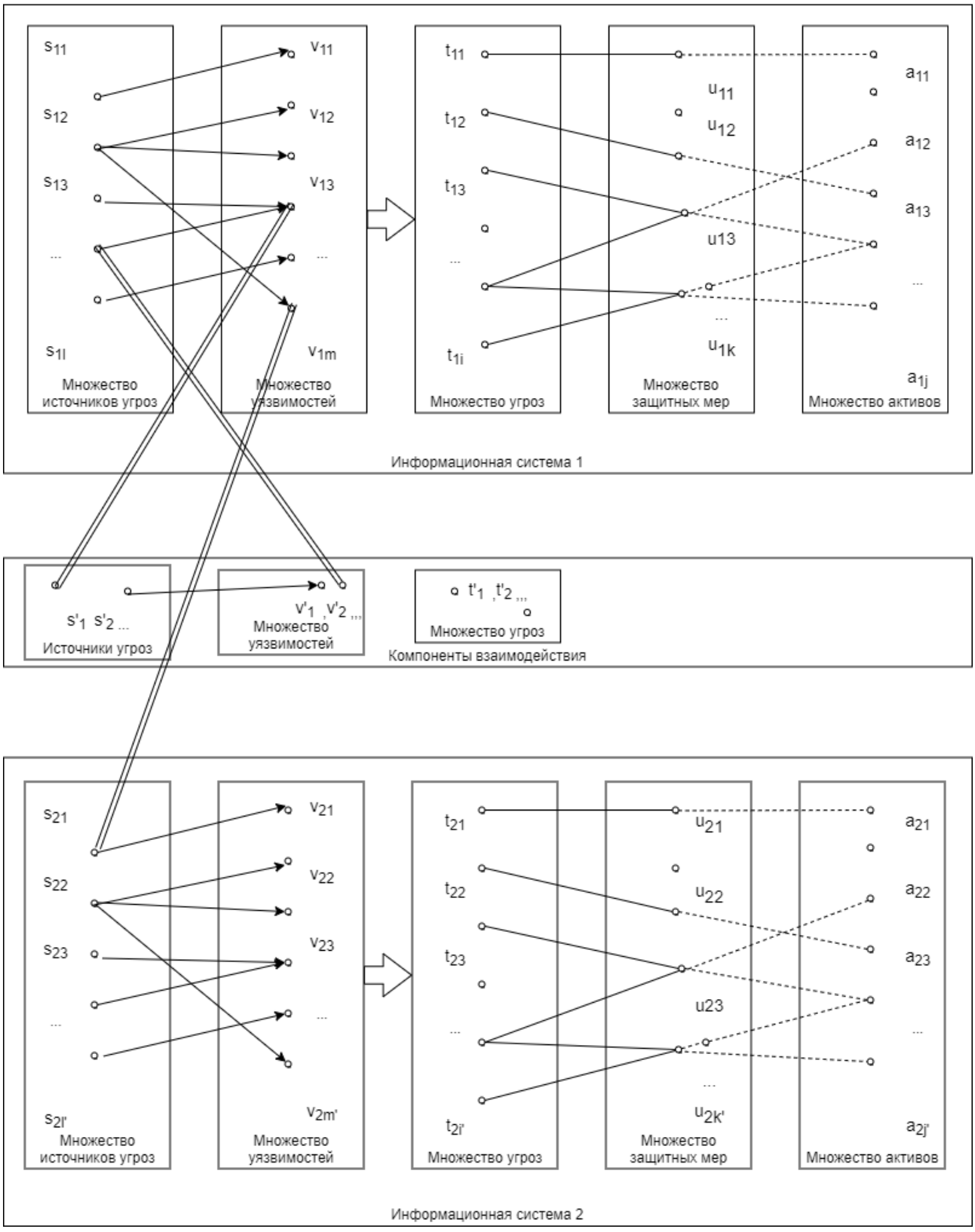

Рис. 2. **Схематическое изображение возникновения новых угроз при организации ИТВ**

Для описания формальной модели ИТВ автоматизированных информационных систем возможно использовать теоретико-множественный подход. Предлагаемая модель ИТВ содержит множество следующих элементов:

$$M_{ИТВ}=\{M_{ТО1}, M_{ИО1}, M_{ПО1}, M_{ИС1}, M_{ТО2}, M_{ИО2}, M_{ПО2}, M_{ИС2}, M_{МВ}\},$$

где M_{TOi} – модель технического обеспечения i-й системы; $M_{ИОi}$ – модель информационного обеспечения i-й системы; $M_{ПОi}$ – модель программного обеспечения; $M_{ИСi}$ – ИТ-сервисы i-й системы; $M_{МВ}$ – модель механизмов взаимодействия.

Модель технического обеспечения при взаимодействии автоматизированных информационных систем:

$$M_{TO}=\langle A_{TO}, K_{APM}, K_{CPB}, K_{TKO}, G_{СТР}\rangle,$$

где A_{TO} – множество всех элементов, составляющих техническое обеспечение автоматизированной информационной системы $A_{TO}=A_{APM}\cup A_{СРВ}\cup A_{ТКО}$ – соответственно, множество элементов АРМ, элементов серверов и элементов телекоммуникационного оборудования (ТКО) автоматизированной системы; $K_{APM}=\{(a^i_{APM},\ \tilde{c}\tilde{c}^i_{APM},\ \tilde{c}\tilde{i}^i_{APM},\tilde{c}\tilde{d}^i_{APM})\}_{i=1}^{N_{APM}}$ – отношение, определяющее связь каждого из АРМ a_i с нечеткими уровнями его конфиденциальности $\tilde{c}\tilde{c}^i_{APM}$, целостности $\tilde{c}\tilde{i}^i_{APM}$ и доступности $\tilde{c}\tilde{d}^i_{APM}$; $K_{CPB}=\{(a^i_{CPB},\ \tilde{c}\tilde{c}^i_{CPB},\ \tilde{c}\tilde{i}^i_{CPB},\tilde{c}\tilde{d}^i_{CPB})\}_{i=1}^{N_{CPB}}$ – отношение, определяющее связь каждого из серверов a_i с нечеткими уровнями его конфиденциальности $\tilde{c}\tilde{c}^i_{CPB}$, целостности $\tilde{c}\tilde{i}^i_{CPB}$ и доступности $\tilde{c}\tilde{d}^i_{CPB}$; $K_{TKO}=\{(a^i_{TKO},\ \tilde{c}\tilde{d}^i_{TKO})\}_{i=1}^{N_{TKO}}$ – отношение, определяющее связь каждого из множества элементов ТКО a_i с нечетким уровнем его доступности $\tilde{c}\tilde{d}^i_{CPB}$; $G_{CTP}=\langle V,E\rangle$ – граф логической структуры технического обеспечения автоматизированной информационной системы, где множество вершин V – элементы автоматизированной системы – серверы и ТКО, а E – множество ребер – кабельные линии связи (например, оптоволокно, витая пара, коаксиальный и др.).

Предложенная формализация логической структуры ИТВ автоматизированных систем в виде графа позволяет отобразить взаимодействие каждого из элементов технического обеспечения в соответствии с заданными уровнями доступности технического обеспечения и предоставляемыми ИТ-сервисами.

Модель информационного обеспечения при взаимодействии автоматизированных информационных систем учитывает взаимодействие информационных активов с учетом их уровней критичности. Следует иметь в виду, что информационные активы хранятся и обрабатываются на АРМ и серверах, а также предоставляются потребителям (в том числе внешней сопрягаемой системе) посредством ИТ-сервисов:

$$M_{ИО}=\langle A_{И}, K_{И}, A_{AC}, A_{ИТ}, R_{ИНФ}, R_{ИТС}, IP\rangle,$$

где $A_И$ – множество информационных активов; $K_{И}=\{(a^i_{И},\ \tilde{c}\tilde{c}^i_{И},\ \tilde{c}\tilde{i}^i_{И},\tilde{c}\tilde{d}^i_{И})\}_{i=1}^{N_{И}}$ – отношение, определяющее связь каждого из информационных активов a_i с нечеткими уровнями его конфиденциальности $\tilde{c}\tilde{c}^i_{И}$, целостности $\tilde{c}\tilde{i}^i_{И}$ и доступности $\tilde{c}\tilde{d}^i_{И}$; $A_{AC}=A_{APM}\cup A_{СРВ}$ – множество активов из состава технического обеспечения, хранящих и обрабатывающих информационные активы; $A_{ИТ}$ – множество ИТ-сервисов автоматизированной системы, участвующих в предоставлении информационных ресурсов множества $A_И$; $R_{ИНФ}: A_И\times A_{AC}\rightarrow\{0,1\}$ – отношение, отображающее участие каждого из элементов множества $A_И$ на множестве A_{AC}; $R_{ИТС}: A_И\times A_{ИТ}\rightarrow\{0,1\}$ – отношение, отображающее предоставление ИТ-сервисом из множества $A_{ИТ}$ информационного актива $A_И$; $IP=\left\{\left(a^i_{И}, a^i_{ИТ}, \{P^i_j\}_{j=1}^{NR}\right)\right\}_{i=1}^{N_{IP}}$ – информационные потоки при интеграции автоматизированных систем на графе G_{CTP}, где $a^i_{И}$ – информационный актив из множества $A_И$; где $a^i_{И}$ – ИТ-сервис автоматизированной информационной системы, предоставляющий на выходе информационный актив (соответствующее значение $R_{ИТС}=1$) P^i_j – маршрут, показывающий движение информации в логической структуре автоматизированных информационных систем.

Модель ИТ-сервисов при взаимодействии автоматизированных информационных систем учитывает организацию предоставления уровней доступности для потребителей. Все

сервисы предоставляются с использованием конкретных элементов множества технического обеспечения и определяются с учетом их доступности:

$$M_{ИТ} = \langle A_{\text{ИТС}}, K_{\text{ИТС}}, G_{\text{ИТС}}, R_{\text{ИТС}} \rangle,$$

где $K_{\text{ИТС}} = \{(a^i_{\text{ИТС}},\ \tilde{c}\tilde{d}^i_{\text{ИТС}})\}_{i=1}^{N_{\text{ИТС}}}$ – отношение, определяющее связь каждого из ИТ-сервисов a_i *с* нечетким уровнем его доступности $\tilde{c}\tilde{d}^i_{\text{И}}$; $G_{ИТС} = \langle A_{\text{ИТС}}, E_{\text{ИТС}} \rangle$ – ориентированный граф, учитывающий зависимость ИТ-сервисов с точки зрения доступности, вершины в котором – ИТ-сервисы из множества $A_{ИТС}$, при этом две вершины в нём связаны ребром, если работоспособность одного из ИТ-сервисов зависит от работоспособности другого; $R_{\text{ИТС}} : A_{ИТС} \times A_{ТО} \rightarrow \{0,1\}$ – отношение, учитывающее зависимость предоставления ИТ-сервиса конкретным элементом технического обеспечения.

Модель механизмов взаимодействия учитывает непосредственное взаимодействие элементов каждой из систем с элементами сопрягаемой системы:

$$M_{\text{МВ}} = \langle A_{\text{МВ}}, G_{\text{МВ}}, R_{\text{МВ}} \rangle,$$

где $A_{МВ}=A_{МВ1} \cup A_{\text{МВ2}}$ – множество информационных активов первой и второй систем, соответственно, непосредственно участвующих в организации ИТВ; $G_{МВ} = \langle A_{\text{МВ}}, E_{\text{МВ}} \rangle$ – ориентированный граф, учитывающий предоставление ИТ-сервисов взаимодействующими активами, при этом направление указывает фактические потоки информации; $R_{\text{МВ}} : A_{МВ} \times A_{ИС} \rightarrow \{0,1\}$ – отношение, учитывающее предоставление активом каждой из систем внешнего ИТ-сервиса.

Таким образом, формальная модель ИТВ, учитывающая модели технического обеспечения, информационного обеспечения, модель ИТ-сервисов и модель механизмов взаимодействия отражает взаимодействие информационных активов, телекоммуникационного оборудования, серверов и АРМ, а также непосредственно ИТ-сервисов.

Для детального определения характера взаимодействия уязвимостей и угроз, возникающих в процессе интеграции автоматизированных систем, может быть применен метод экспертных оценок, в результате которого часть потенциальных уязвимостей может быть признана неэксплуатируемыми. Возможно отнесение отдельных уязвимостей к допустимым (к примеру, не повышающим уровень риска выше допустимого). Вместе с тем возможна ситуация, когда в результате такого анализа будет выявлена одна или несколько уязвимостей, для которых в соответствии с заданным уровнем защищенности потребуются обязательные для применения компенсирующие защитные меры.

Для проведения более точной и эффективной оценки степени значимости угрозы в случаях, когда недостаточно категориальных бинарных значений (есть угроза/нет угрозы), может быть использована шкала, содержащая ряд промежуточных значений. При этом допустимо применение лингвистических переменных в сочетании с нормированием полученных результатов.

Таким образом, приведенные модели в сочетании с последующим использованием метода экспертных оценок позволяют выделять вновь появляющиеся в процессе интеграции актуальные угрозы и проводить их анализ, принимая во внимание оценку относительного совокупного уровня опасности совместной эксплуатации уязвимостей уже существующих в каждой из систем, так и возникших в процессе интеграции. Выбор защитных мер и мероприятий по нейтрализации каждой из выявленных угроз может быть обоснован, исходя из их актуальности и потенциального ущерба [5].

Литература

1. Коваленко Ю.И. Защита информационных технологий: справочник. М.: Русайнс, 2016. 321 с.

2. Коваленко Ю.И., Москвитин Е.И., Тараскин М.М. Методика защиты информации в организациях: монография. М.: Русайнс, 2016. 162 с.

3. Организационно-техническое обеспечение устойчивости функционирования и безопасности сети связи общего пользования / М.В. Буйневич [и др.]. СПб.: СПбГУТ, 2013. 144 с.

4. Буйневич М.В., Израилов К.Е. Антропоморфический подход к описанию взаимодействия уязвимостей в программном коде. Ч. 1: Типы взаимодействий // Защита информации. Инсайд. 2019. № 5 (89). С. 78–85.

5. Основы управления информационной безопасностью: учеб. пособие для вузов / А.П. Курило [и др.]. М.: Горячая линия – Телеком, 2013. 244 с.

References

1. Kovalenko Yu.I. Zashchita informacionnyh tekhnologij: spravochnik. M.: Rusajns, 2016. 321 s.

2. Kovalenko Yu.I., Moskvitin E.I., Taraskin M.M. Metodika zashchity informacii v organizaciyah: monografiya. M.: Rusajns, 2016. 162 s.

3. Organizacionno-tekhnicheskoe obespechenie ustojchivosti funkcionirovaniya i bezopasnosti seti svyazi obshchego pol'zovaniya / M.V. Bujnevich [i dr.]. SPb.: SPbGUT, 2013. 144 s.

4. Bujnevich M.V., Izrailov K.E. Antropomorficheskij podhod k opisaniyu vzaimodejstviya uyazvimostej v programmnom kode. Ch. 1: Tipy vzaimodejstvij // Zashchita informacii. Insajd. 2019. № 5 (89). C. 78–85.

5. Osnovy upravleniya informacionnoj bezopasnost'yu: ucheb. posobie dlya vuzov / A.P. Kurilo [i dr.]. M.: Goryachaya liniya – Telekom, 2013. 244 s.