УДК 004.056.53 DOI: 10.18698/0536-1044-2018-6-86-95

Модель угроз информационной безопасности автоматизированной системы подготовки данных управления летательными аппаратами и модель защиты

А.Г. Андреев[1], Г.В. Казаков[1], В.В. Корянов[2]

[1] ФГБУ «4 ЦНИИ» Минобороны России, 141091, Королев, Российская Федерация, мкр. Юбилейный, ул. М.К. Тихонравова, д. 29
[2] МГТУ им. Н.Э. Баумана, 105005, Москва, Российская Федерация, 2-я Бауманская ул., д. 5, стр. 1

A Model of Threats to Information Security of an Automated Data Preparation System for Aircraft Control and a Model of Protection

A.G. Andreev[1], G.V. Kazakov[1], V.V. Koryanov[2]

[1] Federal State Budgetary Educational Institution 4th Central Scientific Research Institute 4 TsNII, Ministry of Defence of the Russian Federation, 141091, Korolev, Russian Federation, M.K. Tikhonravov St., Bldg. 29
[2] BMSTU, 105005, Moscow, Russian Federation, 2nd Baumanskaya St., Bldg. 5, Block 1

e-mail: kgv.64@mail.ru, kgv.64@mail.ru, vkoryanov@bmstu.ru

При рассмотрении информационной безопасности автоматизированной системы подготовки данных управления летательными аппаратами некоторые факторы риска необходимо перевести в сферу угроз (в частности, угрозу несанкционированного доступа к информации системы). В этом случае можно получить такое описание угроз, которое позволит определить наиболее эффективный способ реализации механизмов защиты в соответствии с требованиями информационной безопасности. С этой целью разработаны модели угроз и защиты, а также новый подход, связанный с комплексным описанием угрозы и средств защиты от ее воздействия. Принципы создания моделей преднамеренных угроз и защиты охватывают основные процедуры реализации угроз и присущи всем их видам. Вербальное описание модели угроз содержит потенциальные источники, способные их реализовать, идентификатор и объект воздействия угрозы, уязвимости, позволяющие осуществить негативные воздействия на защищаемые активы, способы реализации угроз для этих активов, нарушаемые характеристики безопасности защищаемых активов и возможные последствия воздействия угрозы. Приведено как формальное, так и содержательное представление моделей преднамеренных угроз и защиты. Формальное представление основано на использовании плоских графов, для которых определены операции конкатенации и композиции. Содержательное представление включает в себя классификаторы элементов моделей, цели воздействия угрозы в виде нарушения основных свойств информационной безопасности — целостности, конфиденциальности и доступности, а также все виды средств защиты и оценочные уровни доверия.

Ключевые слова: информационная безопасность, классификационная схема, композиция, конкатенация, плоский граф, средства защиты

When reviewing information security of an automated data preparation system for aircraft control, some risk factors need to be raised to the level of threats, namely, the threat of illegal access to system information. In this case, it is possible to obtain a description of threats that could determine the most effective method of implementation of protection mechanisms in accordance with the requirements of information security. For this purpose, models of threats and protection are developed, and a new approach is proposed that involves a comprehensive description of threats and means of protection. The principles of development of the models of premeditated threats and protection incorporate the main procedures of threat realization and are inherent in all the threats. A verbal description of the model of threats contains potential sources capable of realizing the threat, an identifier and an object of impact of the threat, vulnerabilities that can negatively influence securable assets, methods of threat implementation for the securable assets, violated characteristics of safety of the securable assets and possible consequences of the threat impact. Both the formal and the informative presentations of the models of premeditated threats and protection are described. The formal presentation is based on plane graphs, for which concatenations and compositions are defined. The informative presentation contains qualifiers of the model elements, purposes of the threat impact in the form of violation of the main properties of information security such as integrity, confidentiality and accessibility, as well as all types of security features and evaluation trust levels.

Keywords: information security, marking scheme, composition, concatenation, plane graph, security features

При рассмотрении информационной безопасности (ИБ) автоматизированной системы подготовки данных (АСПД) управления летательными аппаратами (ЛА) некоторые факторы риска (в частности, угрозы несанкционированного доступа к информации АСПД) необходимо перевести в сферу угроз ИБ АСПД. В этом случае можно получить такое описание угроз, которое позволит определить самый эффективный способ реализации механизмов защиты в виде средств защиты (СЗ) в соответствии с требованиями ИБ АСПД.

Цель работы — разработка модели угроз (МУ) и связанной с ней модели защиты (МЗ).

В литературе, посвященной ИБ, часто МУ описывают в виде классификации угроз по разным признакам. Например, в работе [1] отмечено, что базовая МУ включает в себя характеристику и классификацию типовых объектов информатизации, классификацию угроз, описание типовых источников угроз, состава и характеристик технических каналов утечки информации.

Аналогичное понимание МУ и МЗ имеет место и во многих других информационных источниках по теории безопасности. Иногда под МУ понимают атаки [2], которые определяются четырьмя элементами (средства реализации атаки–уязвимость–событие безопасности–результат). При этом модель события безопасности включает в себя два элемента (действие–адресат).

Такое представление МУ является более корректным, поскольку в модели задан некоторый порядок действий, приводящий к реализации угрозы. Однако использовать такую МУ для описания любой преднамеренной угрозы нельзя, так как она не построена на основе лексикологической схемы, определяющей логические действия злоумышленника при реализации им любого вида угрозы, и в ней не содержатся признаки классификации элементов этой модели.

В работе [3] основой моделирования процессов нарушения ИБ являлась схема «угроза–источник–метод реализации–уязвимость–ущерб», которую также невозможно использовать в качестве МУ.

Принципы разработки моделей преднамеренных угроз и защиты. При разработке МУ и МЗ следует руководствоваться принципами, которые позволят охватить все основные процедуры реализации угрозы и будут присущи всем их видам. С формальной точки зрения, согласно теореме Понтрягина–Куратовского [4], совокупность МУ и МЗ опишем в виде объединения плоских графов.

Введем понятия конкатенации и композиции плоских графов.

Определение 1. Плоские орграфы U и V образуют конкатенацию, если существует лишь одна дуга, соединяющая любую одну вершину

графа U только с одной вершиной графа V. Процедуру конкатенации обозначим как $U \mapsto V$.

Определение 2. Орграфы U и V_j ($j = 1, 2, \ldots, J$) образуют композицию, если существует более одной дуги, соединяющей вершины графа U с вершинами графа V_j. Процедуру композиции обозначим следующим образом: $U \oplus V$.

Принципы построения формальной МУ и МЗ сводятся к следующим положениям.

1. МУ должна представлять собой плоский линейный граф U, каждая вершина которого связана с его смежной вершиной ровно одной дугой. Плоский линейный граф последовательно соединяет одной дугой все вершины.

2. Вершины плоского линейного графа U должны определяться лексикологической схемой от источника угрозы (начальная вершина U_0) до последствий, к которым может привести реализованная угроза (конечная вершина U_P). Этот принцип обусловлен тем, что лексикологическая схема в виде вершин графа U позволяет воссоздать логический процесс, которым обязательно воспользуется злоумышленник, если создает ту или иную угрозу.

3. Каждая вершина U_p ($p = 1, 2, \ldots, P$) линейного графа U должна представлять собой элемент лексикологической схемы, логически связанный с процессом реализации злоумышленником любой угрозы в информационных ресурсах АСПД.

4. Плоский линейный граф U должен образовывать композицию с некоторыми графами V_j, выполненными в виде классификационных схем лексикологических элементов линейного графа U. Этот принцип обусловлен тем, что каждый элемент лексикологической схемы (вершины графа U) может иметь разное содержание, которое отражается в соответствующей классификационной схеме. Классификационные схемы вершин графа U позволяют учитывать полное множество угроз и выбрать только те из них, которые характерны для АСПД в данный период времени.

Для реализации СЗ АСПД от угрозы любого вида необходимо поставить в соответствие МУ конкретную МЗ, определяемую графом З.

5. Линейный граф U должен составлять конкатенацию с линейным графом З. Единственная дуга, соединяющая вершины графов U и З, относится к идентификатору угрозы, поскольку СЗ, построенные на основе МЗ, должны соответствовать конкретной угрозе с учетом ее особенностей.

6. МЗ, как и МУ, должна представлять собой плоский линейный граф. Этот принцип обусловлен тем, что МЗ строится на основе лексикологической схемы, отражающей все необходимые действия по защите информации от воздействия угроз.

7. Плоский линейный граф З должен образовывать композицию с некоторыми графами M_k ($k = 1, 2, \ldots, K$), выполненными в виде классификационных схем для каждой вершины графа З.

8. МЗ должна учитывать такую особенность, как противодействие угрозе. Этот принцип очевиден, так как он вытекает из назначения МЗ.

9. Исходя из восьмого принципа, МЗ должна содержать двудольный граф Д, вершинами которого служат, с одной стороны, требования ИБ, предъявляемые к СЗ (вершины B_j^* графа Д), с другой — виды СЗ, используемые для противодействия угрозам (вершины B_j^{**} графа Д).

10. МЗ в качестве классификатора должна содержать n-арный линейный граф Z (граф M_2), представляющий собой классификационную схему распределения целей злоумышленника по защищаемым активам (ЗА) АСПД (вершина графа З (цели–активы)), где n — число свойств ИБ, обеспечиваемых средствами защиты. Граф Z должен составлять конкатенацию с вершиной $З_1$ графа З для учета моделью защиты глобальной цели злоумышленника, которая декомпозируется на подцели, связанные с нарушением установленных свойств безопасности для возможных объектов воздействия угроз.

11. В МЗ следует учитывать требования к СЗ противодействия прогнозируемым способам нарушения установленных n-свойств защищаемых активов АСПД (вершины B_j^* графа Д).

12. Очевидно, что в МЗ необходимо учитывать средства противодействия угрозе (вершины B_j^{**} графа Д), связанные с вершинами B_j^*. Поэтому граф Д, учитывающий состав требований к СЗ и соответствующие варианты реализации видов СЗ, должен быть двудольным, включающим в себя вершины B_j^* и B_j^{**} ($B_j^* \bigcap B_j^{**} = \varnothing$). Следовательно, в формальном представлении должна иметь место композиция графов З и Д.

Таким образом, в указанных обозначениях модель преднамеренных угроз–защиты можно записать в формальном виде следующим образом:

$$(V_j \oplus U) \mapsto (M_k \oplus З) \mapsto Z \oplus Д \oplus З.$$

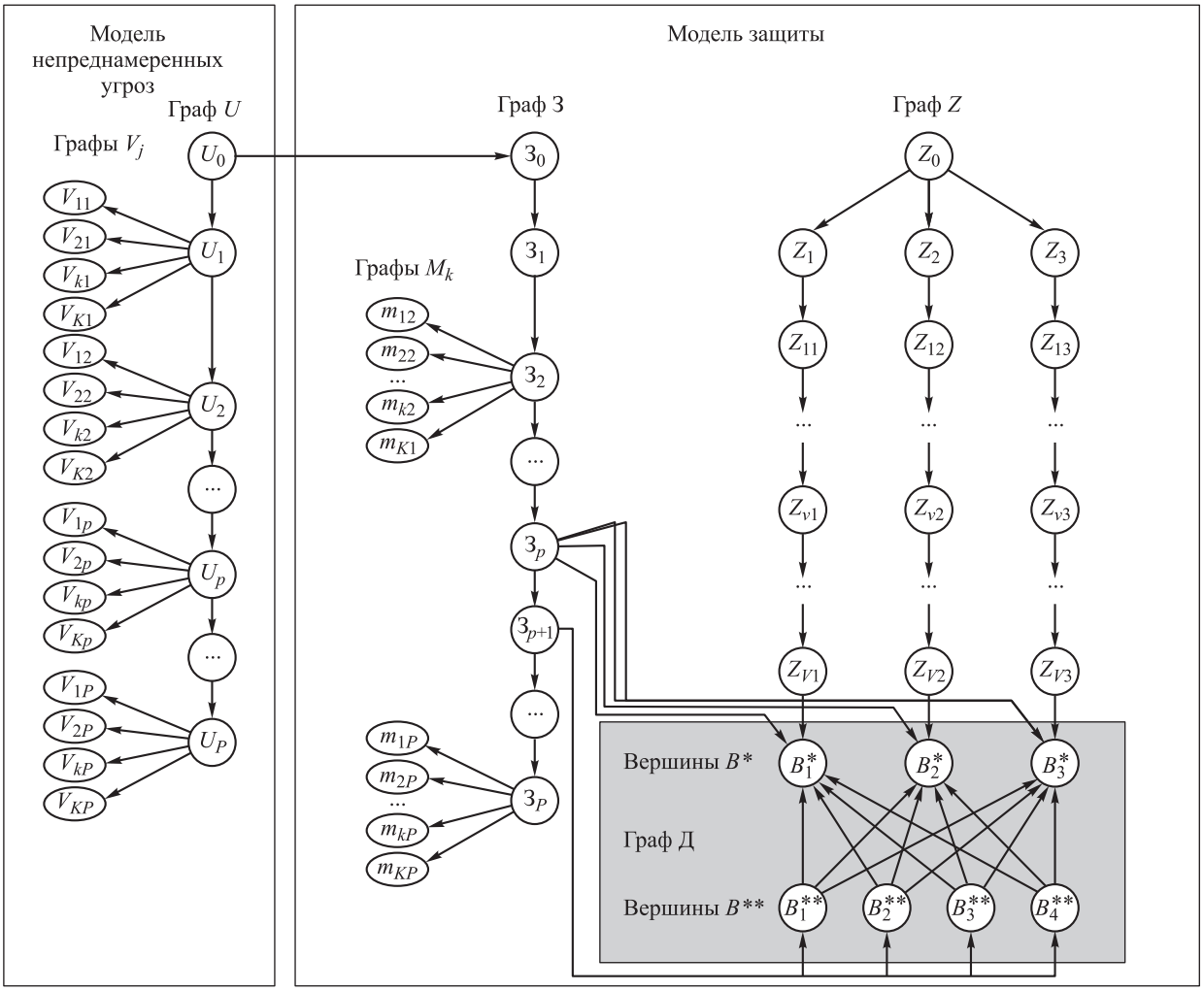

Рис. 1. Формальное представление моделей преднамеренных угроз и защиты

В соответствии с изложенными принципами построения МУ и МЗ формальное описание этих моделей удобно представить в виде соединения графов *U*, З, *Z*, Д, V_j и M_k, как показано на рис. 1.

Модель случайных угроз не содержит мотивированных целей злоумышленника, изощренных способов реализации угрозы, поэтому она значительно проще модели преднамеренных угроз. Средства защиты от случайных угроз достаточно хорошо исследованы и эффективно применяются на практике. По этой причине не имеет смысла разрабатывать ни модель случайных угроз, ни модель защиты от них.

Элементы структуры модели преднамеренных угроз. Чтобы дать конструктивные предложения для реализации механизмов нейтрализации факторов риска АСПД, необходимо перевести факторы риска в сферу угроз ИБ АСПД. Содержательное (вербальное) описание модели преднамеренных угроз в соответствии с ее формальным представлением включает в себя следующие элементы:

- идентификатор угрозы $У_j$ ($j = 1, 2, \ldots, J$);
- потенциальные источники $ИУ_{ij}$, способные реализовать угрозу $У_j$ ($i = 1, 2, \ldots, I$);
- объект воздействия угрозы (защищаемые активы АСПД) $ЗА_d$ ($d = 1, 2, \ldots, D$);
- уязвимости $УЗ_{dm}$, позволяющие осуществить негативные воздействия на $ЗА_d$ ($m = 1, 2, \ldots, M$);
- способы S_{djk} реализации угрозы $У_j$ для активов $ЗА_d$ ($k = 1, 2, \ldots, K$);
- нарушаемые характеристики безопасности $ХБ_{dh}$ ($h = 1, 2, \ldots, H$) защищаемых активов $ЗА_d$;
- возможные последствия воздействия $П_{jr}$ угрозы $У_j$ ($r = 1, 2, \ldots, R$).

Элементы содержательного описания моделей преднамеренных угроз и защиты, приведенные на рис. 2, имеют следующее содержание.

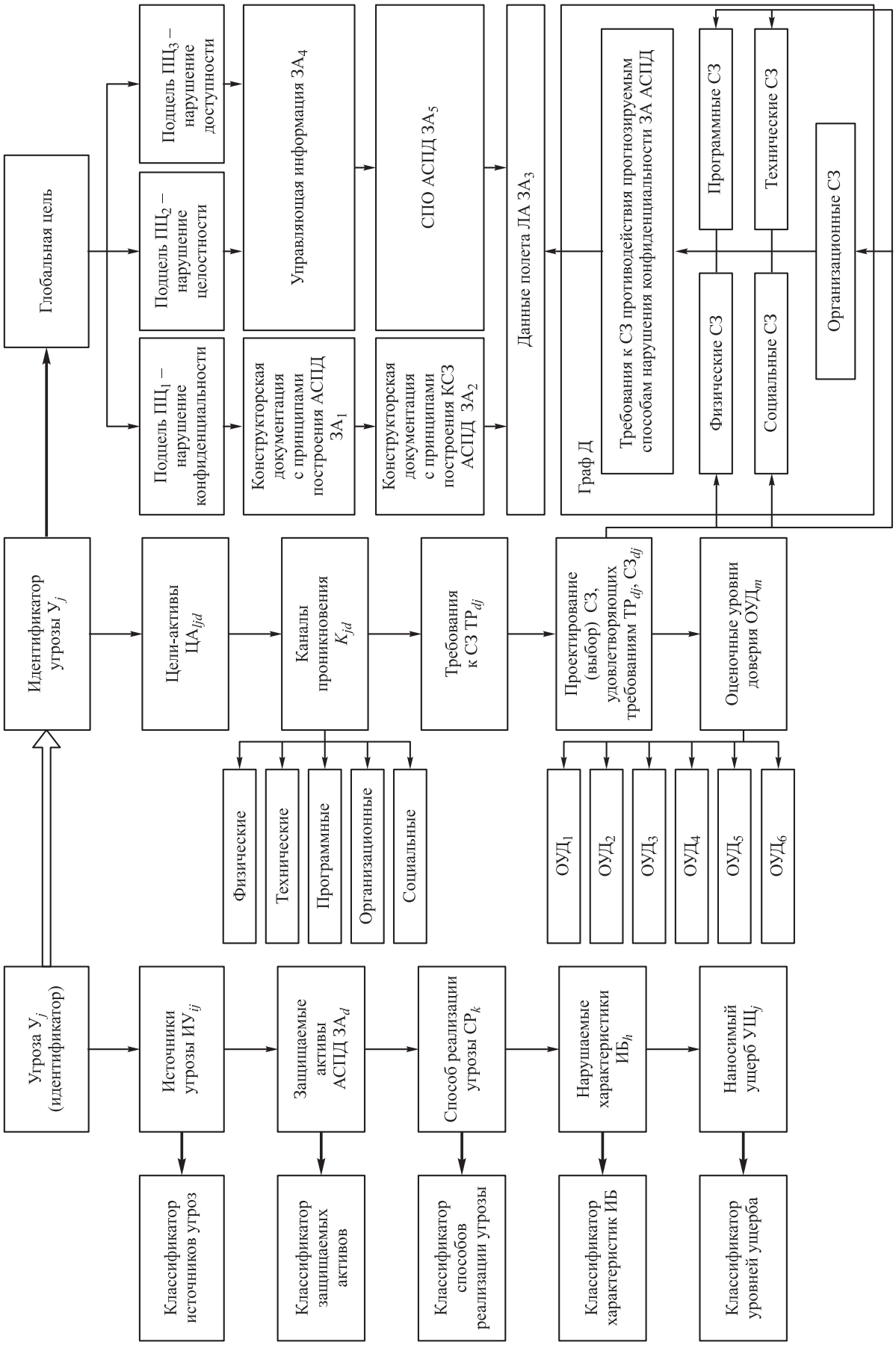

Рис. 2. Содержательное представление моделей преднамеренных угроз и защиты

Идентификатор угрозы предназначен для однозначного представления описываемой угрозы и обеспечения формализованного представления конкретных угроз в их базе данных.

Потенциальные источники угрозы. Преднамеренная угроза $У_j$ может быть реализована несколькими видами источников угроз $ИУ_{ij}$, опасность которых определяется моделью нарушителя [5], включающей в себя такие факторы, как мотивация злоумышленника по созданию угрозы, его квалификация, его вооруженность знаниями об объекте воздействия и средствами реализации угрозы. Состав источников преднамеренных угроз определяется графом V_1, элементы (вершины) которого приведены в таблице.

Выбирается источник угрозы $ИУ^*_{ij}$ с наивысшими мотивацией и квалификацией, т. е. с наивысшим потенциалом реализации угрозы $ПРУ^*_{ijd}$, так как он наиболее опасен, и будет иметь место максимальный риск реализации данной угрозы $У_j$ в защищаемом активе $ЗА_d$ АСПД [6, 7]:

$$ПРУ^*_{ijd} = \max_i \{ПРУ_{ijd}\}.$$

Под термином «нарушитель» понимается лицо, создающее угрозу непреднамеренно (т. е. угроза носит случайный характер), а под термином «злоумышленник» — лицо или группа лиц, создающие преднамеренную угрозу. Классы угроз удобно определять в зависимости от вида источника угрозы. По этому признаку можно выделить классы угроз $КУ_n$ (см. таблицу).

Классы угроз и их источники (элементы графа V_1)

Класс угроз	Источники угроз
$КУ_1$	Случайные угрозы, порожденные внешним или внутренним *объективным* источником угрозы
$КУ_2$	Случайные угрозы, порожденные внешним или внутренним *нарушителем*
$КУ_3$	Преднамеренные угрозы, порожденные внешним или внутренним злоумышленником с *низким* потенциалом нападения
$КУ_4$	Преднамеренные угрозы, порожденные внешним или внутренним злоумышленником со *средним* потенциалом нападения
$КУ_5$	Преднамеренные угрозы, порожденные внешним или внутренним злоумышленником с *высоким* потенциалом нападения
$КУ_6$	Преднамеренные угрозы, порожденные *группой* внутренних или внешних злоумышленников с *высоким* потенциалом нападения

Объект воздействия угрозы. Для достижения своих целей злоумышленник должен установить такой объект $ЗА_d$, воздействие на который позволит ему достичь поставленной цели. Любое воздействие злоумышленника прямым или косвенным образом направлено на определенные виды информационных ресурсов АСПД (защищаемых активов).

Для выработки адекватных мер и СЗ активов АСПД при построении МУ необходимо, во-первых, идентифицировать защищаемые активы $ЗА_d$, во-вторых, проводить их сопоставление с целями потенциального источника угрозы (злоумышленника) и способом реализации им угрозы $У_j$ [8–10] Подверженные воздействию угрозы $У_j$ защищаемые активы определяются спецификой АСПД, использующей изделия информационных технологий (ИТ), и включают в себя конструкторскую документацию с принципами построения системы и ее комплекса средств защиты (КСЗ), управляющую информацию, специальное программное обеспечение (СПО) подготовки данных управления ЛА и данные управления ЛА.

Используемые уязвимости. В соответствии со сценарием реализации угрозы злоумышленник должен обнаружить (или ввести новые) уязвимости в АСПД и ее СЗ, что позволит ему осуществить несанкционированный доступ к защищаемым активам АСПД. Реализация угроз возможна только в случае наличия определенной уязвимости мер безопасности. При этом под уязвимостью понимаются случайным или преднамеренным образом введенные человеком дефекты в элементы АСПД (документацию, персонал, технические средства, программное обеспечение), которые либо сами являются источниками случайных угроз, либо могут использоваться злоумышленником для реализации преднамеренных угроз раскрытия, нарушения целостности или доступности защищаемых активов АСПД.

Способы реализации угрозы. После того как злоумышленник обнаружит (или введет новые) уязвимости, он в зависимости от степени квалификации и вооруженности средствами реализации угрозы может выбрать одну из них и

начать информационную атаку на объект воздействия. Отсюда следует, что важнейшим элементом МУ является определение перечня существующих уязвимостей каждого вида $ЗА_d$ и их средств защиты, в значительной мере предопределяющих способ реализации злоумышленником преднамеренной угрозы. Важно иметь в виду, что реализованная угроза способна сама породить некоторые уязвимости, обнаружение которых основано на детальном анализе возможных каналов доступа к защищаемой информации.

Для АСПД, обрабатывающей информацию конфиденциального характера, необходимо учитывать общий сценарий реализации угрозы, определяющий факторы риска на двух стадиях: предварительного сбора информации и выполнения действий по внедрению в систему с доступом к защищаемым активам. Противодействие этим факторам риска средствами защиты информации АСПД позволит нарушить процесс реализации угрозы и снизить уровень риска ее воздействия до допустимого.

Нарушаемые свойства безопасности активов АСПД. Реализация угрозы направлена на нарушение свойств безопасности защищаемых активов АСПД. В качестве основных свойств ИБ рассматриваются конфиденциальность, целостность, доступность.

Возможные последствия воздействия угрозы. Успешная реализация угрозы влечет за собой последствия, связанные с нарушением безопасного функционирования АСПД. Идентификация таких последствий в рамках МУ позволит проводить ранжирование угроз по степени их опасности, разработки и применения обоснованных и согласованных (взвешенных) организационных, социальных и программно-технических мер и СЗ.

Разработанная структура модели преднамеренных угроз безопасности информации АСПД согласована с документом ФСТЭК России «Безопасность информационных технологий» по всем аспектам, которые необходимо учитывать при анализе угроз безопасности, а также удобна для каталогизации угроз безопасности и разработки структуры МЗ АСПД.

Элементы структуры МЗ. Модель защиты также обеспечивает получение необходимых исходных данных для оценки остаточного риска АСПД как комплексного показателя, определяющего эффективность применяемых мер и средств обеспечения безопасности информации АСПД.

Каждая отдельная угроза — это потенциальная опасность нарушения характеристик безопасности защищаемой информации АСПД, реализация которой возможна в процессе осуществления источником угрозы действий, позволяющих воздействовать на защищаемые информационные ресурсы АСПД. Отсюда следует, что МЗ должна содержать следующие элементы:

- идентификатор угрозы $У_j$, на противодействие которой направлены СЗ;
- цели–активы реализации угрозы $Ц_{dj}$;
- требования, предъявляемые к СЗ информации $Т_{dj}$;
- каналы $К_{jd}$ проникновения угрозы $У_j$ к защищаемой информации $ЗА_d$;
- проектируемое (или выбираемое) изделие ИТ в виде средств защиты $СЗ_{dhj}$ активов $ЗА_d$ АСПД от воздействия угрозы $У_j$;
- оценочный уровень доверия $ОУД_m$ средств защиты активов $ЗА_d$.

Перечисленные структурные элементы МЗ имеют следующее содержание. Идентификатор угрозы $У_j$, выбираемый из ее описания в структуре модели преднамеренных угроз, служит отправным пунктом для нахождения СЗ от данного вида угрозы. Цели–активы реализации угрозы $У_j$ определяются только путем прогнозирования. При этом необходимо учитывать вид источника угрозы (обладающего наивысшим потенциалом ее реализации), целью которого является нарушение хотя бы одного из трех основных свойств ИБ: целостности, конфиденциальности, доступности.

В зависимости от подцели злоумышленника он может использовать в качестве объекта нападения следующие защищаемые активы АСПД: конструкторскую документацию с принципами построения АСПД и ее КСЗ, управляющую информацию, СПО АСПД и данные управления ЛА.

Задача проектирования КСЗ АСПД заключается в построении такой системы, которая обеспечивала бы требуемое качество процесса подготовки данных управления ЛА в условиях воздействия угроз безопасности подготовленных данных [11, 12]. При этом КСЗ следует проектировать в соответствии с моделью защиты для установленного актуального состава преднамеренных угроз.

Каналы $К_{jd}$ проникновения угрозы $У_j$ к защищаемым активам $ЗА_d$ должны содержать

все возможные виды каналов: физические, технические, программные, организационные и социальные. При этом необходимо учитывать каналы не только непосредственного проникновения угрозы к защищаемым активам, но и позволяющие создать источник внедрения преднамеренной угрозы (например, внедрить агента в состав персонала АСПД или завербовать кого-либо из действующих лиц из состава персонала АСПД).

Требования к СЗ информации $ТР_{dj}$ должны соответствовать таковым, предъявляемым к безопасности автоматизированной системы, изложенным в утвержденных документах ФСТЭК, с учетом ее специфики и актуального состава угроз.

Проектируемое (или выбираемое) изделие ИТ в виде средства защиты $СЗ_{dhj}$ активов $ЗА_d$ АСПД от воздействия угрозы $У_j$ должно относиться к одному из типов (физические, технические, программные, организационные, социальные) или их комбинации в зависимости от возможных каналов проникновения угрозы и выявленных уязвимостей.

Оценочные уровни доверия $ОУД_m$ к СЗ информационных ресурсов АСПД должны соответствовать классу защищенности АСПД. Доверие — основа уверенности в том, что изделие ИТ отвечает целям безопасности [5]. Для получения доверия необходимо провести активное исследование — оценку (сертификационных испытаний) изделия ИТ, используемого в составе СЗ информации. Уровень доверия определяется пакетом его требований. В работе [5] определены пакеты требований доверия — оценочные уровни доверия $ОУД_m$ (m = 1, 2, …, 7). Для АСПД следует применять $ОУД_6$, так как уровень доверия $ОУД_7$ практического использования к настоящему времени не нашел.

Выводы

1. В состав свойств, определяющих качество АСПД, входит такое комплексное свойство, как ИБ, определяющее степень защиты информационных ресурсов АСПД от воздействия угроз несанкционированного доступа к защищаемым активам АСПД.

2. Из теории безопасности известно, что качественную защиту информационных ресурсов АСПД от воздействия угроз можно осуществить только с помощью МУ и МЗ. В предлагаемом формальном представлении модели преднамеренных угроз и соответствующей МЗ заложены принципы построения, охватывающие все основные действия злоумышленника при реализации им любой преднамеренной угрозы.

3. Для разработки МУ и МЗ использован математический аппарат теории плоских графов. Определены понятия конкатенации и композиции плоских графов, которые позволили объединить МУ и МЗ формальным путем.

Литература

[1] Минаков В. *Базовая модель угроз безопасности совместным информационным ресурсам (проект) ЗАЩИТА-БР*. Воронеж, ГНИИИ ПТЗИ, 2003. 111 с.

[2] Лукацкий А. *Обнаружение атак*. Санкт-Петербург, BHV-СПб, 2003. 608 с.

[3] Вихорев С.В. *Методические рекомендации по проведению анализа и оценки возможностей реализации угроз информационной безопасности на объекте*. Москва, Элвис, 2001. 32 с.

[4] Харари Ф. *Теория графов*. Москва, Мир, 2003. 297 с.

[5] ГОСТ Р ИСО/МЭК 15408-3–2013. *Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 3. Компоненты доверия к безопасности*. Москва, Стандартинформ, 2014. 267 с.

[6] Глухов А.П., Котяшев Н.Н., Купцов А.В. Оценка чувствительности ресурсов и рисков применения систем критических приложений к влияющим факторам. *Стратегическая стабильность*, 2007, № 1, с. 39–44.

[7] Василенко В.В., Корнеев В.В., Котяшев Н.Н. Аналитические представления процессов риска в комплексах и системах критических приложений. *Двойные технологии*, 2002, № 1, с. 20–24.

[8] Быков А.Ю., Алтухов Н.О., Сосенко А.С. Задача выбора средств защиты информации в автоматизированных системах на основе модели антагонистической игры. *Инженер-*

ный вестник МГТУ им. Н.Э. Баумана, 2014, № 4. URL: http://engbul.bmstu.ru/doc/708106.html (дата обращения 15 января 2018).

[9] Быков А.Ю., Гуров А.В. Задача выбора средств защиты информации от атак в автоматизированных системах при нечетких параметрах функции цели. *Инженерный журнал: наука и инновации. МГТУ им. Н.Э. Баумана*, 2012, № 1. URL: http://engjournal.ru/catalog/it/hidden/86.html (дата обращения 15 января 2018).

[10] Быков А.Ю., Панфилов Ф.А., Шмырев Д.В. Задача выбора средств защиты в автоматизированных системах с учетом классов защищенности от несанкционированного доступа к информации. *Инженерный журнал: наука и инновации. МГТУ им. Н.Э. Баумана*, 2012, № 1. URL: http://engjournal.ru/catalog/it/hidden/85.html (дата обращения 15 января 2018).

[11] Быков А.Ю., Артамонова А.Ю. Модификация метода вектора спада для оптимизационно-имитационного подхода к задачам проектирования систем защиты информации. *Наука и образование. МГТУ им. Н.Э. Баумана*, 2015, № 1. URL: http://technomag.bmstu.ru/doc/754845.html (дата обращения 15 января 2018).

[12] Сидак А.А. Композиционный подход к формированию требований к изделиям, реализующим функции безопасности в информационных системах семейства профилей защиты. *Стратегическая стабильность*, 2010, № 4, с. 42–48.

References

[1] Minakov V. *Bazovaia model' ugroz bezopasnosti sovmestnym informatsionnym resursam (proekt) ZAShchITA-BR* [The basic model of threats to the safety joint information resources (draft) PROTECTION-BR]. Voronezh, GNIII PTZI publ., 2003.111 p.

[2] Lukatskii A. *Obnaruzhenie atak* [Intrusion detection]. Saint-Petersburg, BHV-SPb publ., 2003.608 p.

[3] Vikhorev S.V. *Metodicheskie rekomendatsii po provedeniiu analiza i otsenki vozmozhnostei realizatsii ugroz informatsionnoi bezopasnosti na ob"ekte* [Methodical recommendations on carrying out the analysis and an assessment of possibilities of implementation of threats of information security on object]. Moscow, Elvis publ., 2001.32 p.

[4] Kharari F. *Teoriia grafov* [Graph theory]. Moscow, Mir publ., 2003. 297 p.

[5] *GOST R ISO/MEK 15408-3–2013. Informatsionnaia tekhnologiia.Metody i sredstva obespecheniia bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologii. Ch. 3. Komponenty doveriia k bezopasnosti* [State Standard 15408-3–2013. Information technology. Security techniques. Evaluation criteria for IT security. Part 3. Security assurance requirements]. Moscow, Standartinform publ., 2014. 267 p.

[6] Glukhov A.P., Kotiashev N.N., Kuptsov A.V. Otsenka chuvstvitel'nosti resursov i riskov primeneniia system kriticheskikh prilozhenii k vliiaiushchim faktoram [Estimation of sensitivity of resources and risks of application of systems of critical applications to influencing factors]. *Strategicheskaia stabil'nost'* [Strategic Stability]. 2007, no. 1, pp. 39–44.

[7] Vasilenko V.V., Korneev V.V., Kotiashev N.N. Analiticheskie predstavleniia protsessov riska v kompleksakh i sistemakh kriticheskikh prilozhenii [Analytical representations of risk processes in complexes and systems of critical applications]. *Dvoinye tekhnologii* [Dual technologies]. 2002, no. 1, pp. 20–24.

[8] Bykov A.Iu., Altukhov N.O., Sosenko A.S. Zadacha vybora sredstv zashchity informatsii v avtomatizirovannykh sistemakh na osnove modeli antagonisticheskoi igry [The task of selecting the means of information protection in automated systems based on the antagonistic game model]. *Inzhenernyi vestnik MGTU im. N.E. Baumana* [Engineering Bulletin of the BMSTU.]. 2014, no. 4. Available at: http://engbul.bmstu.ru/doc/708106.html (accessed 15 January 2018).

[9] Bykov A.Iu., Gurov A.V. Zadacha vybora sredstv zashchity informatsii ot atak v avtomatizirovannykh sistemakh pri nechetkikh parametrakh funktsii tseli [A Problem on Choosing Protection against Attacks in Automated Systems with Fuzzy Parameters of Goal Function]. *Inzhenernyi zhurnal: nauka i innovatsii. MGTU im. N.E. Baumana* [Engineering Journal: Science and Innovation]. 2012, no. 1. Available at: http://engjournal.ru/catalog/it/hidden/86.html (accessed 15 January 2018).

[10] Bykov A.Iu., Panfilov F.A., Shmyrev D.V. Zadacha vybora sredstv zashchity v avtomatizirovannykh sistemakh s uchetom klassov zashchishchennosti ot nesanktsionirovannogo dostupa k informatsii [A Problem on Choosing Protection in Automated Systems Taking into Account the Classes of Immunity against Unauthorized Data Access]. *Inzhenernyi zhurnal: nauka i innovatsii. MGTU im. N.E. Baumana* [Engineering Journal: Science and Innovation]. 2012, no. 1. Available at: http://engjournal.ru/catalog/it/hidden/85.html (accessed 15 January 2018).

[11] Bykov A.Iu., Artamonova A.Iu. Modifikatsiia metoda vektora spade dlia optimizatsionno-imitatsionnogo podkhoda k zadacham proektirovaniia system zashchity informatsii [A Modified Recession Vector Method Based on the Optimization-Simulation Approach to Design Problems of Information Security Systems]. *Nauka i obrazovanie. MGTU im. N.E. Baumana* [Science & Education. Bauman MSTU]. 2015, no. 1. Available at: http://technomag.bmstu.ru/doc/754845.html (accessed 15 January 2018).

[12] Sidak A.A. Kompozitsionnyi podkhod k formirovaniiu trebovanii k izdeliiam, realizuiushchim funktsii bezopasnosti v informatsionnykh sistemakh semeistva profilei zashchity [Composed approach for formation of the requirements for products that realize security functions in information systems. families of protection profiles]. *Strategicheskaia stabil'nost'* [Strategic Stability]. 2010, no. 4, pp. 42–48.

Статья поступила в редакцию 11.04.2018

Информация об авторах

АНДРЕЕВ Анатолий Георгиевич (Королев) — кандидат технических наук, старший научный сотрудник. ФГБУ «4 ЦНИИ» Минобороны России (141091, Королев, Российская Федерация, мкр. Юбилейный, ул. М.К. Тихонравова, д. 29, e-mail: kgv.64@mail.ru).

КАЗАКОВ Геннадий Викторович (Королев) — кандидат технических наук, доцент, начальник управления ФГБУ «4 ЦНИИ» Минобороны России, почетный работник науки и техники Российской Федерации (141091, Королев, Российская Федерация, мкр. Юбилейный, ул. М.К. Тихонравова, д. 29, e-mail: kgv.64@mail.ru).

КОРЯНОВ Всеволод Владимирович (Москва) — кандидат технических наук, доцент, первый заместитель заведующего кафедрой «Динамика и управление полетом ракет и космических аппаратов». МГТУ им. Н.Э. Баумана (105005, Москва, Российская Федерация, 2-я Бауманская ул., д. 5, стр. 1, e-mail: vkoryanov@bmstu.ru).

Information about the authors

ANDREEV Anatoliy Georgievich (Korolev) — Candidate of Science (Eng.), Senior Researcher. Federal State Budgetary Educational Institution 4th Central Scientific Research Institute 4 TsNII, Ministry of Defence of the Russian Federation (141091, Korolev, Russian Federation, M.K. Tikhonravov St., Bldg. 29, e-mail: kgv.64@mail.ru).

KAZAKOV Gennadiy Viktorovich (Korolev) — Candidate of Science (Eng.), Associate Professor, Head of Department. Federal State Budgetary Educational Institution 4th Central Scientific Research Institute 4 TsNII, Ministry of Defence of the Russian Federation (141091, Korolev, Russian Federation, M.K. Tikhonravov St., Bldg. 29, e-mail: kgv.64@mail.ru).

KORYANOV Vsevolod Vladimirovich (Moscow) — Candidate of Science (Eng.), Associate Professor, First Deputy Department Head, Dynamics and Flight Control of Rockets and Space Vehicles. Bauman Moscow State Technical University (105005, Moscow, Russian Federation, 2nd Baumanskaya St., Bldg. 5, Block 1, e-mail: vkoryanov@bmstu.ru).

Просьба ссылаться на эту статью следующим образом:
Андреев А.Г., Казаков Г.В., Корянов В.В. Модель угроз информационной безопасности автоматизированной системы подготовки данных управления летательными аппаратами и модель защиты. *Известия высших учебных заведений. Машиностроение*, 2018, № 6, с. 86–95, doi: 10.18698/0536-1044-2018-6-86-95.

Please cite this article in English as:
Andreev A.G., Kazakov G.V., Koryanov V.V. A Model of Threats to Information Security of an Auto-mated Data Preparation System for Aircraft Control and a Model of Protection. *Proceedings of Higher Educational Institutions. Machine Building*, 2018, no. 6, pp. 86–95, doi: 10.18698/0536-1044-2018-6-86-95.