УДК 004.056

В.И. Черныш

Харьковский национальный университет радиоэлектроники, Харьков

МОДЕЛЬ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ ОРГАНИЗАЦИИ ВОЗДУШНОГО ДВИЖЕНИЯ

Предлагается унифицированная модель управления рисками информационной безопасности в системе организации воздушного движения. Данная модель удовлетворяет международным нормативным документам и особенностям построения информационно-телекоммуникационных систем организации воздушного движения и их компонентам.

Ключевые слова: *метод, риски информационной безопасности, система организации воздушного движения.*

Введение и постановка задачи исследования

Вопрос об управлении рисками информационной безопасности (ИБ) становится все более актуальным. Сегодня построение и эффективная эксплуатация систем информационной безопасности невозможны без анализа и управления рисками информационной безопасности такой системы. Основной задачей данного направления является объективная идентификация угроз и оценка наиболее значимых информационных рисков для организации, а также адекватность используемых средств контроля рисков в целях повышения эффективности и рентабельности предприятия.

Анализ рисков ИБ – систематическое использование информации для идентификации источников и оценки величины риска [1 – 3]. Анализ рисков служит основой для оценивания рисков, обработки и принятия рисков.

Оценивание риска ИБ – процесс сравнения оценочной величины риска с установленными критериями риска с целью определения уровня значимости риска [2].

Основными задачами оценки рисков информационной безопасности являются:

1) выбор необходимых требований и средств защиты от угроз ИБ;

2) принятие своевременных решений относительно применения средств защиты;

3) правильная расстановка приоритетов в выборе механизмов обеспечения ИБ;

4) оценка экономической целесообразности и эффективности мер, обеспечивающих ИБ;

5) избежание кризисных ситуаций, которые могут иметь негативное влияние на функционирование информационно-телекоммуникационной системы.

Целью статьи является разработка модели управления рисками ИБ системы организации воздушного движения.

Изложение основного материала

Анализ проблемы управления рисками информационной безопасности в системе организации воздушного движения

Система организация воздушного движения представляет собой сложную систему, включающую информационно-телекоммуникационную систему организации воздушного движения (ИТС ОрВД) и субъектов системы ОрВД (персонал). На рис. 1 представлены компоненты системы ОрВД.

Рис. 1. Компоненты системы ОрВД

Информационные активы провайдера АНО являются объектом для многих видов угроз. Угроза может стать причиной нежелательного инцидента, в результате которого провайдеру будет причинен ущерб.

Этот ущерб может возникнуть в результате атаки на программные и аппаратные ресурсы ИТС ОрВД, что приведет к несанкционированному раскрытию, модификации, повреждению, уничтожению информации в ИТС ОрВД.

Информационно-телекоммуникационная система организации воздушного движения (ИТС ОрВД) – совокупность информационных систем и телекоммуникационных сетей, обеспечивающих деятельность критически важного объекта гражданской авиации (провайдера АНО), основной задачей которого является обеспечение безопасности воздушного движения. ИТС ОрВД, включает компоненты, такие как автоматизированные системы управления воздушным движением (АС УВД), системы наблюдения за воздушной обстановкой, приемные и передающие центры, автоматизированные системы полетно-информационного обслуживания (АС ПИО), системы авиационной фиксированной связи и телефонии.

Угрозы ИБ могут быть осуществлены посредством использования уязвимостей системы.

Уязвимости представляют собой слабости защиты, ассоциированные с информационными активами провайдера АНО. Эти слабости могут использоваться одной или несколькими угрозами, являющимися причиной нежелательных инцидентов, которые могут стать причиной нестабильного функционирования компонентов ИТС ОрВД. Уязвимости – это любые факторы, делающие возможной успешную реализацию угроз. Можно с уверенностью констатировать, что уязвимости являются основной причиной возникновения атак. Наличие же слабых мест в ИТС ОрВД может быть обусловлено самыми различными факторами, начиная с простой халатности сотрудников и заканчивая преднамеренными действиями злоумышленников.

Управление рисками ИБ в системе ОрВД как научная и управленческая деятельность представляет собой совокупность последовательных этапов научно-практических исследований, направленных на определение достоверных и обоснованных характеристик риска, а также на выявление эффективных мер по его сокращению [4].

Анализ существующих подходов к проблеме управления рисками сложных систем показывает, что этот вопрос в большей степени является открытым, так как сама эта проблемная область еще плохо формализована и изучена. Модели этой проблемной области очень неточны, дают, как правило, качественные оценки, достоверность которых не всегда очевидна. Это связано со сложностью самой проблемы и с ее зависимостью от чисто субъективных факторов. Для описания таких моделей используется различный математический аппарат: методы субъективной вероятности, нечеткие множества, нейронные сети и т.д. Подобные модели являются средством уменьшения степени неопределенности при выборе возможных вариантов решений задач управления рисками.

При управлении рисками в сложных системах, таких как система ОрВД, у экспертов всегда возникают трудности при анализе рисков, а если их число велико и они плохо структурированы, то линейное ранжирование рисков и выбор среди них наиболее значимого превращается в сложную задачу. Лимит времени, отводимого на аудит информационной безопасности корпоративных систем, необходимость учета нечисловых характеристик системы защиты информации требуют разработки новых подходов к ее решению. Возможный выход из создавшегося положения заключается в использовании в качестве основной процедуры сравнения и оценки сценариев метода парных сравнений [3 – 5].

В статье предлагается модель управления рисками ИБ системы ОрВД (рис. 2), которая удовлетворяет международным стандартам в области управления информационной безопасности, а также учитывает особенности построения и функционирования ИТС ОрВД.

В соответствии с международными стандартами [5] управление рисками ИБ провайдером АНО предполагает следующее:

1) определение основных целей и задач защиты информационных активов провайдера АНО;

2) создание эффективной системы оценки и управления рисками ИБ.

Модель оценки рисков ИБ может быть адаптирована к большинству типов провайдеров АНО и их структурных подразделений (центров обслуживания воздушного движения). Предложенная модель управления рисками ИБ включает в себя следующие этапы и модели:

1) оценка рисков информационной безопасности;

2) модель атак на ИТС ОрВД;

3) анализ угроз информационной безопасности в ИТС ОрВД;

4) модель оптимального выбора комплекса средств защиты;

5) модель выбора оптимальной ИТС ОрВД.

Модель атак на информационно-телекоммуникационную систему организации воздушного движения

Атаки на ИТС ОрВД могут быть подразделены на внешние и внутренние. Внешние сетевые атаки проводятся извне с узлов, которые не входят в состав ИТС ОрВД. Внутренние атаки проводятся с одного из компонентов ИТС ОрВД, например АС УВД.

Потенциальными целями злоумышленников могут выступать рабочие станции, серверы, коммуникационное оборудование, а также каналы связи ИТС ОрВД. При этом если атака проводится по сети, то она может быть соотнесена с одним из пяти уровней модели ВОС.

Атаки могут носить однонаправленный или распределенный характер. Распределенные атаки в

отличие от однонаправленных проводятся одновременно из нескольких источников. Примером таких атак служат распределенные атаки типа «отказ в обслуживании», которые реализуются путем формирования и одновременной посылки из нескольких источников большого числа паке заданных узлам, являющимся объектами атаки.

Для наглядности модели управления рисками информационной безопасности (рис. 2) необходимо построить математическую модель атак на ИТС ОрВД. Построение такой модели является одним из этапов управления рисками ИБ.

Проведенные исследования существующих типов моделей атак на ИТС позволили констатировать, что созданные в настоящее время модели могут быть классифицированы по следующим базовым критериям [4 – 6]:

1) степень формализуемости модели;

2) тип представления модели;

3) возможность расширения модели;

4) возможность учета в модели последовательности действий, совершаемых нарушителем в процессе проведения информационной атаки;

5) уровень детализации модели.

Рис. 2 .Унифицированная модель управления рисками ИБ

Рассмотрим обобщенную математическую модель атаки на ИТС ОрВД [6], которая базируется на следующих трех основных множествах: V – множество уязвимостей ИТС ОрВД, A – множество методов реализации атак и C – множество последствий атак. Для описания взаимосвязи между элементами множества A, V и C определим отношение W на множестве $U=A\times V\times C$. Принадлежность элемента (a, v, c) отношению W, где $a \in A$, $v \in V$, $c \in C$, интерпретируется следующим образом: «Атака на ИТС

ОрВД, реализуемая нарушителем методом а путем активизации уязвимости v и приводящая к последствию с».

С каждой уязвимостью $v_i \in V$ связано множество A_i, являющееся подмножеством множества А и включающее атаки на ИТС ОрВД, направленные на активизацию уязвимости v_i . При этом $0<|A_i|<|A|$, т.е. одна уязвимость v_i не может быть активизирована для реализации всех атак из множества А. Вместе с тем не существует такой уязвимости, на основе которой не могло быть реализовано ни одной атаки на ИТС ОрВД.

С каждой атакой на ИТС ОрВД $a_j \in A$ связано множество V_j, являющееся подмножеством V и включающее уязвимости, активизируемые атакой a_j. При этом $0<|V_i|<|V|$, т.е. одна атака a_j не может активизировать одновременно все уязвимости ИТС ОрВД, и, наоборот, не существует такой атаки, которая бы не активизировала ни одной уязвимости АС.

С каждой атакой $a_j \in A$ связано множество C_j, являющееся подмножеством множества С и включающее последствия атаки a_j. При этом $0<| C_i| <|C|$, т.е. атака a_j не может привести одновременно ко всем последствиям, входящим во множество С, и, вместе с тем, атака a_j не может не иметь ни одного последствия.

С каждым последствием реализации атаки на ИТС ОрВД $c_k \in C$ связано множество A_k, являющееся подмножеством множества А и включающее атаки, приводящие к последствию c_k. При этом $0<|A_k| <|A|$, т.е. не существует такого последствия, к которому бы не привело ни одной атаки, и в то же самое время, последствие не может быть следствием реализации всех атак, входящих в множество А.

Анализ защищаемых информационных ресурсов

Информационные ресурсы можно определить как весь имеющийся объем информации в рассматриваемой информационно-телекоммуникационной системе.

В настоящее время ИТ достигли такого уровня развития, когда объемы информации и уровень ее сложности потребовали создания информационной индустрии. Наличие информации определяет развитие организации. Информация стала стратегическим ресурсом, а информационные ресурсы являются одними из важнейших.

На этапе анализа рисков ИБ (рис. 2) – анализ защищаемых информационных ресурсов определяют множество информационных ресурсов ИТС ОрВД – D, которые должны быть защищены от возможных атак нарушителей. Элементами этого множества могут являться: файловые ресурсы; служебные данные, хранящиеся в СУБД; пользовательские документы и др. Выбор защищаемых ресурсов должен осуществляться исходя из состава той информации, которая необходима для выполнения функциональных задач ИТС ОрВД. В множество D также должны входить информационные ресурсы, защита которых должна быть обеспечена в соответствии в отечественной правовой базой. Одноэтапные информационные ресурсы могут объединяться в рамках одного элемента множества D.

На рис. 3 представлена структура информационных ресурсов.

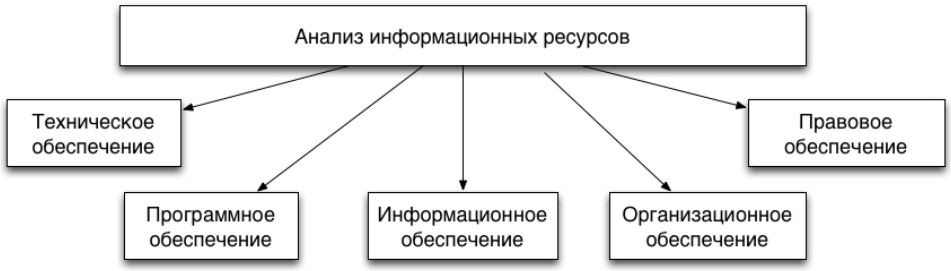

Рис. 3. Структура информационных ресурсов

Техническое (аппаратное) обеспечение ИТС ОрВД – комплекс технических средств, устройств и процессов, позволяющих использовать и осуществлять управление информационными ресурсами провайдером АНО.

Программное обеспечение ИТС ОрВД – использование математических средств для работы с информационными ресурсами, программные продукты и техническая документация по их использованию [7, 8].

Информационное обеспечение ИТС ОрВД – комплекс классификации и кодирования информации, унификации систем документооборота, схемы движения информации и методология построения базы данных.

Организационное обеспечение ИТС ОрВД – приемы и методы взаимодействия между сотрудниками провайдера АНО и техническими средствами по вопросу управления информационными ресурсами.

Правовое обеспечение информационно-телекоммуникационной системы ОрВД – совокупность нормативно-правовых актов, регулирующих вопросы возникновения, перемещения и эксплуатации информационных ресурсов провайдера АНО.

Для проведения эффективной оценки рисков ИБ необходимо детально проанализировать аппаратное и программное обеспечение.

Анализ программного и аппаратного обеспечения

На этапе анализа программного и аппаратного обеспечения метода оценки рисков ИБ (рис. 2) формируются два множества: S – множество программного обеспечения и H – множество аппаратного обеспечения, которое используется в ИТС ОрВД для хранения и обработки информационных ресурсов, входящих в множество D (рис. 4).

Для того чтобы задать взаимосвязь между аппаратным обеспечением ИТС ОрВД и установленным на нем программным обеспечением, вводится бинарное отношение B_1, определенное на множестве $U_1=S\times H$. При этом принадлежность элемента (s,h) отношению B_1, где $s \in S$, $h \in H$, интерпретируется следующим образом: «программное обеспечение s, установленное на аппаратном обеспечении h». Далее определяется взаимосвязь между элементами множеств D, S и H при помощи тернарного отношения B_2, заданного на множестве $U_2= D \times S \times H$. Принадлежность элемента (d, s, h) отношению B_2, где $d \in D$, $s \in S$, $h \in H$, интерпретируется следующим образом: «Информационный ресурс d, обрабатываемый средствами программного обеспечения s, которое установлено на аппаратном обеспечении h». В случае, если информационный ресурс обрабатывается только аппаратным обеспечением, например, коммутатором, взаимосвязь между элементами множеств D и H можно определить через бинарное отношение B_3, заданное на множестве $U_3= D \times H$. На основе отношений B_1, B_2, B_3 формируется таблица, состоящая из следующих полей: порядковый номер элемента таблицы, наименование аппаратного обеспечения, перечень установленного на нем программного обеспечения и список информационных ресурсов, которые хранятся или обрабатываются программно-аппаратным обеспечением ИТС ОрВД. Необходимо отметить, что в некоторых случаях на аппаратном обеспечении может отсутствовать программное обеспечение, если оно интегрировано в аппаратные компоненты устройства. Это характерно, например, для некоторых коммутаторов и маршрутизаторов, используемых в АС УВД, логика работы которых реализована на аппаратном уровне в виде специализированных микросхем [5].

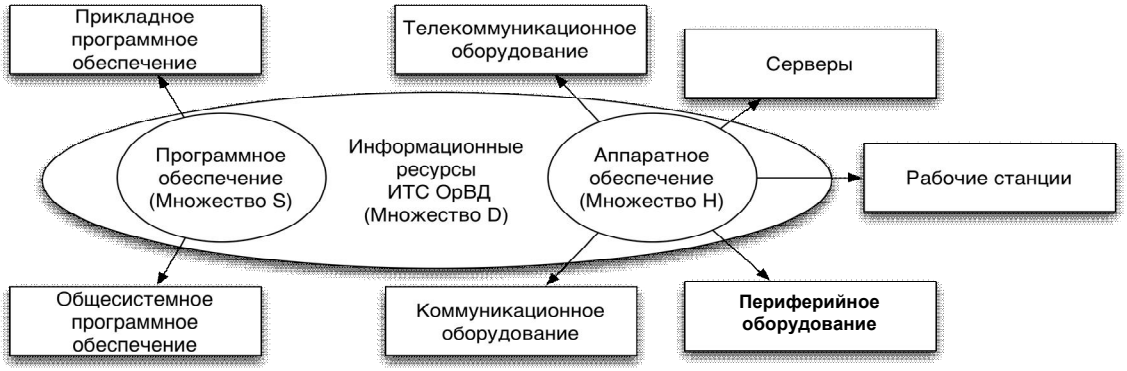

Рис. 4. Анализ множеств и их компонентов в методе оценки рисков ИБ

Анализ информационных потоков

На этапе анализа информационных потоков определяется множество категорий пользователей ИТС ОрВД – U, а также права доступа этих пользователей к информационным ресурсам множества D (рис. 5).

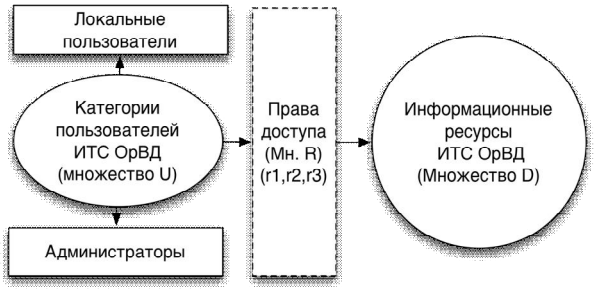

Рис. 5. Связь между пользователями и информационными ресурсами ИТС ОрВД

Категории пользователей формируются на основе организационной структуры провайдера АНО, а также функциональных обязанностей его сотрудников. Возможные права пользователей по доступу к информации определяются в множестве R, которое, как минимум, включает в себя три следующих элемента: r_1 – доступ к информационному ресурсу только на чтение данных, r_2 – доступ к информационному ресурсу только на запись данных, r_3 – доступ к информационному ресурсу на чтение и на запись данных.

Для того чтобы указать, какие права доступа к информации имеют категории пользователей, определяется тернарное отношение B_4, заданное на множестве $U_4= U \times D \times R$. При этом принадлежность элемента (u, d, r) отношению B_4, где $u \in U$, $d \in D$, $r \in R$, интерпретируется следующим образом: «Кате-

гория пользователей u имеет доступ к информационному ресурсу d с правами r». На основе отношения B_4 формируется таблица, содержащая следующие поля: порядковый номер элемента таблицы, категория пользователей ИТС ОрВД, список информационных ресурсов и прав доступа к ним [6 – 8].

Идентификация существующих комплексов средств защиты

На данном этапе определяется множество комплексов средств защиты Z, которые используются в ИТС ОрВД. В множество Z включаются как организационные меры, так и технические средства защиты. После этого формируется бинарное отношение B_5, определенное на множестве $U_5 = Z \times D$. Принадлежность элемента (z, d) отношению B_5, где $z \in S$, $d \in D$, интерпретируется следующим образом: «Средство z предназначено для защиты информационного ресурса d». Одно средство защиты $z \in Z$ может использоваться для зашиты одновременно нескольких информационных ресурсов, и, наоборот, один информационный ресурс может защищаться одновременно несколькими средствами защиты [6 – 8].

На основе отношения B_5 формируется таблица, содержащая следующие поля: порядковый номер элемента таблицы, информационные ресурсы ИТС ОрВД, а также перечень средств их защиты. Взаимоотношение между элементами множеств D, S, H и Z показано на рис. 6.

Рис. 6. Схема взаимосвязи между элементами множеств D, S, H и Z

Оценка уязвимостей на основе собранных данных

Уязвимости могут присутствовать как в программно-аппаратном, так и в организационно-правовом обеспечении ИТС ОрВД. Характерно, что основная часть уязвимостей организационно-правового обеспечения обусловлена отсутствием у провайдера АНО и его структурных подразделений нормативных документов, качающихся вопросов информационной безопасности. В качестве примера уязвимости данного типа может служить отсутствие в организации утвержденной концепции или политики информационной безопасности, которые бы определяли требования к защите ИТС ОрВД и ее компонентов, а также конкретные пути их реализации [7 – 8]. Организационно-правовые уязвимости имеют место и в тех случаях, когда существующие нормативно-правовые документы не полностью охватывают все необходимые аспекты защиты от информационных атак или же когда такие документы существуют лишь на бумаге и не внедряются в практику [8].

Уязвимости программно-аппаратного обеспечения могут присутствовать в программных или аппаратных компонентах рабочих станций пользователей ИТС ОрВД, серверов, а также коммуникационного оборудования и каналов связи системы ОрВД.

Уязвимости могут существовать как на технологическом, так и на эксплуатационном этапах жизненного цикла ИТС ОрВД и ее компонентов. На технологическом этапе нарушителями могут стать инженерно-технические работники, участвующие в процессе проектирования, разработки, установки и настройки программно-аппаратного обеспечении ИТС ОрВД. Анализ уязвимостей ИТС ОрВД представлен на рис. 7.

Оценка вероятности проведения атак

На этапе оценки вероятности проведения атак анализ рисков определяется вероятностью того, что в случае проведения атак на защищаемые ресурсы могут быть успешно преодолены все средства защиты, используемые в ИТС ОрВД. Для этого для каждого информационного ресурса $d \in D$ разрабатываются графовые модели возможных атак, направленных на нарушение конфиденциальности, целостности или доступности ресурса. Графовые модели создаются рабочей группой, приводящей анализ рисков, на основе ранее составленных множеств D, S, H и Z , а также отношений B_1, B_2, B_3, B_4, B_5.

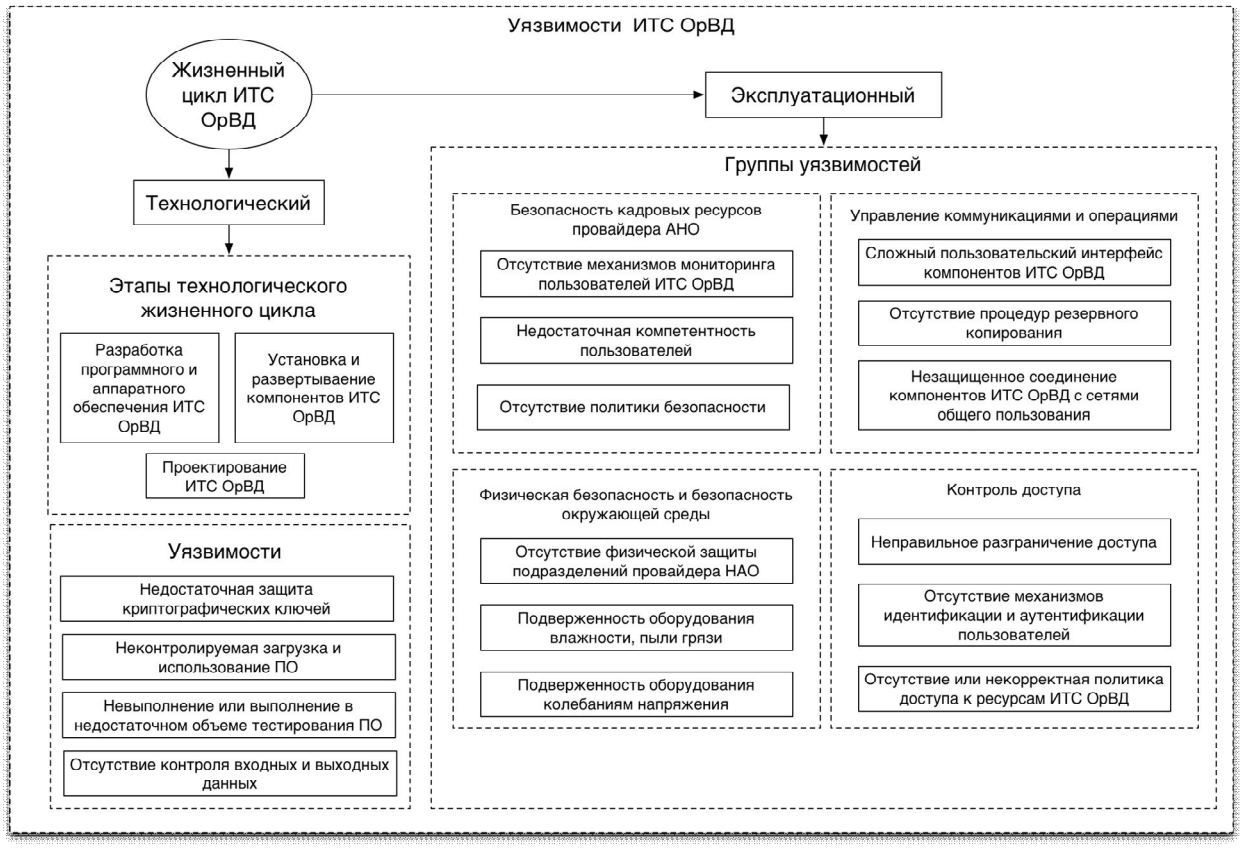

Рис. 7. Анализ уязвимостей ИТС ОрВД

Каждая модель атаки представляет собой граф G=<L, E>, где L – множество вершин, а E – множество дуг гарафа G. Для графа G определено отношение $T \in \{E \times W\}$, которое каждой дуге из множества E ставит в соответствие один или несколько элементов отношения W, что позволяет интерпретировать каждую дугу $e \in E$ как один из этапов развития атаки.

Для каждого графа составляется множество путей G_p , в котором каждый путь $g_p=(e_{p1}, e_{p2}, e_{p3},\ldots., e_{pn})$, $e_{pn} \in E$, $g_p \in G_p$ описывает один из возможных сценариев развития атаки. Так, например, для графа G, изображенного на рис. 8, множество G_p включает два элемента, и, таким образом, описывает два возможных сценария атаки $G_p=\{(e_1), (e_3 , e_2)\}$.

$T=\{ (e_1, (a_2, v_1, c_3)),\quad (e_2, (a_1, v_3, c_3)),\quad (e_3, (a2, v_3, c_1).$

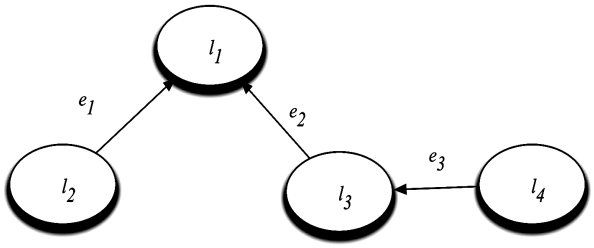

Рис. 8. Пример графа атаки на ИТС ОрВД

Оценка ущерба в случае нарушения услуг информационной безопасности

Этап анализа рисков ИБ предполагает оценку ущерба L, который может быть нанесен в случае успешной атаки на информационные ресурсы из множества D. Оценка ущерба проводится по отношению к возможным последствиям атаки – нарушением конфиденциальности, целостности или доступности информационного ресурса. Модель предусматривает использование как количественных, так и качественных шкал для определения уровня ущерба. Количественные шкалы предполагают оценку математического ущерба по десятибалльной системе. При этом каждый балл шкалы должен соответствовать определенному уровню материальных потерь, которые может понести организация в случае проведения успешной атаки на ресурс.

При использовании качественных шкал ущерб оценивается по пяти понятийным уровням – «малый ущерб», «умеренный ущерб», «ущерб средней тяжести», «большой ущерб», «критический ущерб». При оценке ущерба необходимо учитывать возможную потерю репутации компании, финансовые потери, правовые и судебные штрафы и др. Уровень ущерба определяется не членами рабочей группы, проводящей анализ рисков, а представителями организации, в ведении которой находится исследуемая ИТС ОрВД.

В результате проведения пятого этапа оценки рисков формируется таблица, состоящая из следующих полей: порядковый номер элемента таблицы, информационный ресурс из множества D, тип последствия атаки на этот ресурс и уровень ущерба L.

Расчет значения рисков информационной безопасности

На данном этапе вычисляется значение риска R на основе ранее определенного уровня ущерба и вероятности атак. Для каждого защищаемого информационного ресурса d ∈ D могут вычисляться три значения риска: риск нарушения конфиденциальности, целостности и доступности информационных ресурсов ИТС ОрВД. Значение риска может определяться по количественной или качественной шкале оценки. В случае применения количественной шкалы риск вычисляется по шкале как произведение значений ущерба и вероятности атаки, которые были определены на пятом и шестом этапах оценки, соответственно – $R_{ij} = P(G_j)\cdot L_j$, $i = \overline{1,...,|D|}$, $j = \overline{1,...,3}$. На этом завершается процесс оценки рисков, после которого следует процедура анализа полученных значений и разработка рекомендаций по минимизации значений рисков информационной безопасности.

Заключение

Риск информационной безопасности ИБ информационно-телекоммуникационной системы представляет собой интегральную оценку того, насколько эффективно существующие средства защиты способны противостоять информационным атакам. Процесс анализа рисков включает три основных этапа: этап сбора исходной информации об ИТС, этап оценки рисков на основе собранных данных и этап разработки рекомендаций по управлению выявленными рисками информационной безопасности ИТС.

Предложенная в статье модель управления рисками информационной безопасности ИТС ОрВД может быть внедрена в концепцию информационной безопасности аэронавигационного провайдера как унифицированная.

Данная модель разработана в соответствии с международными стандартами в области управления информационной безопасностью, такими как ISO/IEC 27005:2010 и регулятивных требований по безопасности системы ОрВД.

Кроме того, предложенная модель включает в себя общепринятые подходы в оценке рисков ИБ (например, метод анализа иерархий), однако, адаптирован к ИТС ОрВД.

Список литературы

1. Замула О.А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О.А. Замула, В.І. Черниш // Системи обробки інформації : збірних наукових праць. – Х.: ХУ ПС, 2011. – Вип. 2(92). – С. 53-56.

2. Черныш В.И. Методы оценивания информационных рисков компании / В.И.Черныш // Материалы XV Международного юбилейного молодёжного форума «Радиоэлектроника и молодежь в XXI веке»: Сб. тезисов, 18–20 апреля 2011 р., Т.5. – Х.: ХНУРЭ, 2011. – С. 195.

3. ISO 27005 ISO/IEC 27005:2010. Information technology. Security techniques. Information security risk management – ISO / IEC, 2010. – 70 p.

4. Сердюк В.А. Анализ современных тенденций построения моделей информационных атак / В.А. Сердюк // Информационные технологии. – 2004. – № 5. – С. 94-101.

5. Замула А.А. Концептуализация информационных процессов в системе организации воздушного движения / А.А. Замула, В.И. Черныш, Ю.В. Землянко // Вісник Національного університету «Львівська політехніка»: «Автоматика, вимірювання та керування». – Львів: Львівська політехніка, 2013. – №774. – С. 21-27.

6. Сердюк В.А. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий. – М.: Высшая Школа Экономики (Государственный Университет), 2011. – 576 с.

7. Замула А.А. Автоматизация процессов обслуживания воздушного движения / А.А. Замула, А.В. Северинов, В.И. Черныш // Наука і техніка Повітряних Сил Збройних Сил України: Науково-технічний журнал. – Х.: ХУ ПС, 2013. – № 2(6). – С. 161-165.

8. Замула А.А. Эффективность информационных процессов и технологий при обслуживании воздушного движения / А.А. Замула, В.И. Черныш, Ю.В. Землянко // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: ХУ ПС, 2013. – Вип. 2(35). – С. 89-93.

Поступила в редколлегию 10.12.2015

Рецензент: канд. техн. наук, доцент О.В. Сєвєрінов, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

МОДЕЛЬ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗЕПЕКИ В СИСТЕМІ ОРГАНІЗАЦІЇ ПОВІТРЯНОГО РУХУ

В.І. Черниш

Пропонується уніфікована модель управління ризиками інформаційної безпеки в системі організації повітряного руху. Дана модель задовольняє міжнародним нормативним документам та особливості побудови інформаційно-телекомунікаційних систем організації повітряного руху та їх компонентам.

Ключові слова: *метод, ризики інформаційної безпеки, система організації повітряного руху.*

MODEL RISK MANAGEMENT INFORMATION SECURITY AIR TRAFFIC MANAGEMENT SYSTEM

V.I. Chernysh

Proposed unified governance model information security risks in the system of air traffic management. This model meets international regulations and characteristics of information-telecommunication systems of air traffic and their components.

Keywords: *method of information security risks, system of air traffic management.*