ПОВЫШЕНИЕ «УСТОЙЧИВОСТИ» РЕГЛАМЕНТОВ ДЕЯТЕЛЬНОСТИ КАК СПОСОБ ПРОТИВОДЕЙСТВИЯ НЕУМЫШЛЕННОМУ ИНСАЙДИНГУ

Буйневич М. В.[1], Моисеенко Г. Ю.[2]

DOI: 10.21681/2311-3456-2024-6-108-116

Цель исследования: *обеспечение безопасности информационных ресурсов организации от угрозы неумышленного инсайдинга за счет повышения «устойчивости» регламентов деятельности сотрудников.*

Методы исследования: *системный анализ, аналитическое моделирование, синтез, гипотетический эксперимент, программная инженерия.*

Полученные результаты: *получена графоаналитическая модель предметной области – неумышленного инсайдинга, разработан пошаговый метод синтеза устойчивых регламентов деятельности и архитектура программного комплекса моделирования инструкций; предполагается, что эти научные результаты на данный момент не имеют релевантных аналогов. Теоретическая значимость работы состоит в переводе деятельности, традиционно описываемой на естественном языке, в аналитическую плоскость. Практическая же значимость определяется применением каждого из результатов для повышения безопасности защищаемых информационных ресурсов в практически любой организации, связанной с информационными технологиями.*

Научная новизна *состоит в том, что впервые в качестве уязвимости организации рассматривается «неустойчивость» регламентов деятельности сотрудников (инструкций), а в качестве источника угрозы безопасности информационных ресурсов – девиация поведения сотрудников, вследствие чего происходит отклонение от шагов инструкции.*

Ключевые слова: *информационные ресурсы, регламент деятельности, неумышленный инсайдинг, угроза безопасности, способ противодействия, моделирование.*

Введение

Обеспечение сохранности информационных ресурсов (далее – ИР) является важнейшим аспектом функционирования любой организации; особенно это критично для организаций, обеспечивающих устойчивое функционирование и безопасность государства. ИР таких организаций могут подвергаться целому пулу деструктивных воздействий различной природы – программной, технической, иной. Однако особое место среди них занимают те, которые исходят изнутри самого защищаемого периметра, поскольку источник угрозы в этом случае уже формально преодолел ряд защитных мер. Характерным направлением такого рода угроз является инсайдинг, суть которого заключается в неправомерной деятельности сотрудников организации против своих же защищаемых ИР; как правило, с целью незаконного овладения информацией, которая является собственностью организации.

При этом инсайдеров можно поделить на два типа: заведомо заинтересованного в неправомерных действиях (например, если он был внедрен или завербован враждебным государством или конкурирующей организацией) [1], и легального сотрудника – несознательно (неосознанно) нарушившего инструкции, что привело к возникновению инцидента с ИР (например, если он по халатности раскрыл конфиденциальную информацию) [2]. Второй тип инсайдерства – неумышленного – в некоторой степени даже опаснее первого, поскольку такой сотрудник соответствует практически всем критериям отбора (не замечен в подозрительных связях, лоялен, ответственен, не склонен к… и проч.) и не может быть выявлен при приеме на работу или при регулярных контрольных проверках.

Ситуация еще более усложняется, если легальный сотрудник в принципе выполняет все действия строго по инструкциям и допускает на первый взгляд незначительную «оплошность», которая, однако, приводит к катастрофическим последствиям; такая ситуация описывается в теории катастроф, как прохождение точки бифуркации. Однако, нисколько не оправдывая сотрудника, для недопущения подобных ситуаций необходимо учитывать человеческий фактор, которому подвержены абсолютно все субъекты, обладающие разумом, эмоциями, психикой и другими аспектами, отсутствующими у автомата. И если устранение подобных субъективных уязвимостей в самом человеке находится в зоне ответственности психологических

1 Буйневич Михаил Викторович, доктор технических наук, профессор, профессор кафедры прикладной математики и информационных технологий Санкт-Петербургского университета государственной противопожарной службы МЧС России, Санкт-Петербург. ORCHID: https://orcid.org/0000-0001-8146-0022. Scopus Author ID: 56122749800. E-mail: bmv1958@yandex.ru

2 Моисеенко Григорий Юрьевич, руководитель направления Министерства обороны РФ, Москва, Россия. E-mail: mogreq@mail.ru

и иных социальных наук, то альтернативное решение стоит искать в более организационно-технической составляющей предметной области.

Причины неумышленного инсайдерства

Базовый анализ предметной области [3–6] показывает, что причина возникновения неумышленного инсайдерства со стороны благонадежных сотрудников может лежать в плоскости формирования «небезопасных» должностных и/или иных регламентирующих деятельность инструкций, по сути, представляющих собой совокупность (в более строгом смысле – граф) переходов субъекта и окружающей системы (на которую он влияет) между некоторыми состояниями. При этом, ошибочный переход в иное состояние, не указанное в инструкции, в результате может привести к иному развитию всего «пути» субъекта и, как результат, к попаданию в состояние, характеризуемое нарушениями конфиденциальности, целостности и доступности ИР. Одной из основных причин такой ситуации является близость состояний, позволяющая субъекту (в т.ч. под влиянием внешних воздействий, изменяющих его внутренние факторы) выполнить ошибочное действие, перейдя тем самым в незапланированное состояние.

Поясним данную идею на следующем примере, который будет являться «сквозным» для статьи. Предположим, что высококвалифицированный, опытный и благонадёжный сотрудник в процессе выполнения должностных обязанностей получает документ с конфиденциальными сведениями в пункте «A» и переносит его в пункт «B». При этом он проходит около помещения «C». В случае строгого и автоматического выполнения инструкций, сотрудник походит мимо помещения «C», перенеся документ из начальной в конечную точку.

Однако, исходя из того, что сотрудник является человеком, то он обладает собственной целенаправленной активностью, связанной с мыслительной деятельностью, потребностями, ощущениями и пр. Как результат, он может «зайти» в помещение «C» (например, если это столовая или место для курения – в зависимости от повышенных потребностей сотрудника), по небрежности оставить там документ, выйти из помещения и продолжить выполнение инструкции вплоть до пункта «B». Естественно, пропажа документа в момент посещения помещения «C» может быть достаточно оперативно обнаружена (например, если его сдача контролируется другими сотрудниками или техническими средствами), однако документ будет находиться в «небезопасном» состоянии время, которое сотрудник затратит на движение из «C в «B». При этом необходимо отметить, что уже, как только документ покинул пункт «A» и до тех пор, пока он оказался в пункте «B», его безопасность (даже в условиях нахождения в руках человека) была снижена – например, вследствие потенциально возможного физического или иного воздействия на сотрудника.

Примечание. Следует говорить о снижении/повышении именно *уровня* безопасности, так как применительно к безопасности более корректно «обеспечена – не обеспечена» или нарушена. Именно так следует трактовать понятие «безопасность» применительно к ИР и, в частности, конфиденциальным документам.

Таким образом, часть ответственности за нарушение безопасности (в данном случае – возможности раскрытия конфиденциальной информации) лежит на непродуманной инструкции сотрудника [7] в рамках конкретной организации (поскольку, если между пунктами «A» и «B» проходит полностью изолированный коридор, то шанс попадания документа третьим лицам будет минимальным).

Анализ нарушения для приведенного примера позволяет выдвинуть две следующие его «глубинные» причины. Во-первых, очевидную – физическое расположение «C», близкое к месту, через которое проходит маршрут сотрудника из «A» в «B», создает потенциальную возможность отклонения им от регламентированной траектории. А, во-вторых, скрытую – возможности, предоставляемые помещением «C», оказываются близкими к потенциальным потребностям, присущим сотруднику; такой сотрудник может объяснить свои действия фразами «захотелось перекусить» или «покурить».

Исходя из приведенного (и достаточно показательного) примера можно выделить проблему предметной области в форме противопоставления потребностей и возможностей следующим образом. С одной стороны, от сотрудников организации требуется выполнения инструкций, безопасное по отношению к ИР. С другой стороны, наличие человеческого фактора приводит к девиации поведения сотрудников (т.е. отхождение от пользовательских паттернов [8]), вследствие чего происходит отклонение от шагов инструкции, что может приводить к угрозе безопасности ИР [9]. Исходя из того, что эффективность противодействия самой сути человека является в некотором смысле спорной, то возможным разрешением противоречия может являться снижение вероятности угрозы путем повышения «устойчивости» инструкций к их нарушению сотрудником под воздействием внутренних (т.е. человеческих) факторов (вызванных, в том числе и внешними).

Говоря простым языком, требуется создание таких инструкций, которые бы заданная группа сотрудников в данной организации не смогла бы нарушить, а в идеале – даже нарушив, но незначительно, не смогла бы создать угрозу безопасности ИР. Для примера выше, инструкция может быть модифицирована отдалением пути перемещения документа

с конфиденциальными сведениями от потенциально-опасных помещений.

Альтернативные способы в примере, такие, как перенесение помещения «С» или разнесение времени работы с документами и режима открытия помещения «С», хотя и «имеют место быть», но в статье не рассматриваются, т.к. являются в разы более ресурсозатратными и имеющими в целом негативное влияние на общее функционирование организации. Повышения же устойчивости инструкций к неумышленному инсайдингу можно достичь, предоставив для начала аппарат оценки их безопасности. Как результат, руководитель (ответственное за безопасность должностное лицо) сможет варьировать содержание инструкций, их параметры и порядок действий сотрудников для достижения сценариев поведения, наиболее безопасных с позиции ИР (даже в условиях «нулевого доверия» [10]).

В интересах разрешения противоречия указанным способом предложим достаточно каноническую методологическую трехэтапную схему исследования с получением соответствующих научных результатов (в кавычках):

1. Анализ предметной области с получением «Аналитической модели неумышленного инсайдинга» (далее – Модель), взаимоувязывающей в формализованном виде элементы организации, инструкции, параметры (т.е. внутренние факторы) сотрудников и их характеристики (т.е. влияние на выполняемые регламентированные действия), ИР и их безопасность;
2. Создание «Метода структурно-параметрического синтеза и оценки устойчивости инструкций» (далее – Метод), позволяющей построить Модель, задать ее параметры, а также произвести оценки инструкций с позиции безопасности ИР;
3. Разработка «Архитектуры программного комплекса моделирования устойчивости инструкций», представляющей собой многослойное описание (с позиции логических модулей, информационных объектов, алгоритмов и т.п.) реализации Метода, функционирующего на базе Модели; за этим следует разработка соответствующего прототипа (далее – Прототип), базовое тестирование которого покажет работоспособность Метода и адекватность Модели.

По завершении указанных этапов исследования потребуется произвести оценку полученных результатов, например, путем моделирования реально произошедших инцидентов по причине нарушения инструкций сотрудниками организации и установления возможности и точности выявления (идентификации и локализации) потенциально возможных нарушений.

Опишем далее гипотетическое (на данный момент исследования) представление ожидаемых результатов на каждом этапе, указав способы их реализации.

Этап 1. Аналитическая модель

На первом этапе требуется провести анализ предметной области на предмет определения основных ее онтологических сущностей и их связей. Так, очевидно, что основными сущностями будут следующие: структура конкретной организации, защищаемые ИР, инструкции, сотрудники, безопасность. К вторичным сущностям можно отнести уточняющие основные, а именно следующие: внутренние факторы сотрудников и выполняемые в рамках инструкций действия, состояния сотрудников (с позиции выполнения инструкций), состояния защищаемых ИР, переходы между состояниями и влияние на безопасность.

Анализ онтологической модели позволит формализовать все ее сущности и их связи в виде соответствующей аналитической модели, что будет первым научным результатом. Идея такой модели может строиться на следующих предпосылках.

Во-первых, инструкции, хотя и описаны, как правило, в достаточно общем виде, однако их выполнение происходит на конкретной структуре организации (например, если в организации принципиально отсутствует работа с конфиденциальными документами в бумажном виде, то их перенос из пункта «А» в «В» невозможен в принципе).

Во-вторых, выполнение сотрудником действий, указанных в инструкции, приводит к его переходу в другое состояние (например, выполнив действие согласно инструкции по переходу из «А» в «В», сотрудник поменяет пространственную характеристику с координаты «А» на координату «В»).

В-третьих, последовательность перемещения сотрудника между состояниями влияет также и на ИР, и в особенности те, к которым применяется инструкция (например, выход сотрудникам из пункта «А» с документом приводит к некоторому снижению безопасности последнего, а посещение сотрудником помещения «С», в котором, по внутреннему регламенту, все документы должны быть временно оставлены без присмотра и вовсе приводит к реальной предпосылке утечки конфиденциальной информации).

Следуя указанным предпосылкам, можно переложить действия из примера на Модель в графическом представлении. Предположим, что должностная инструкция звучит, как «Сотрудник должен получить документ в пункте «А», перенести его в пункт «В» и сдать там на хранение». Также учтем специфику структуры организации, заключающуюся в расположении помещения «С» на пути следования из «А в «В».

Таким образом, можно ввести следующие состояния сотрудника:

«W» (*аббр. от англ.* Workplace, *перев. на русс.* Рабочее Место) – штатное расположение сотрудника в организации (например, рабочий кабинет);
«A» – нахождение сотрудника в пункте «A» до получения документа;
«A'» – нахождение сотрудника в пункте «A» после получения документа;
«T'» (*аббр. от англ.* Temporary, *перев. на русс.* Временное Место) – нахождение сотрудника, имеющего с собой документы, около помещения «C»;
«B'» – нахождение сотрудника в пункте «B» до сдачи документа;
«B» – нахождение сотрудника в пункте «B» после сдачи документа.

Аналитически, состояния могут быть записаны следующим образом:

$$P \in \{W, A, A', T', B', B\},$$

где P (*аббр. от англ.* Position, *перев. на русс*. Место, локация) – некоторое (пространственное) состояние сотрудника.

Наличие показателей у каждого из состояний, позволяющих описывать их в едином пространстве, может быть записано следующим образом:

$$\begin{cases} i \in I \\ N = |I| \\ P \equiv \langle P^1 \ldots P^i \ldots P^N \rangle \end{cases}$$

где i – показатель, I – множество всех показателей, N – количество всех показателей (как мощность множества I), P^i – значение i-го показателя состояния.

«Безопасное» моделирование выполнения инструкции представлено на Рисунке 1 – сценарий 1; обозначение «[ ]» означает состояние документа: «+» – документ у сотрудника, «–» – документ не у сотрудника.

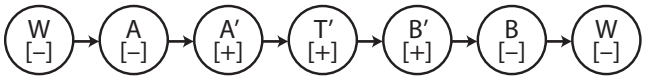

Рис. 1. Пример моделирования «безопасного» выполнения инструкции

Так, следуя Рисунку 1, в некоторый момент времени (состояние «A' [+]») документ оказывается у сотрудника, а в последующий (состояние «B' [–]») он переходит в хранилище.

Аналитически, такие переходы между состояниями могут быть записаны следующим образом:

Сценарий 1: $W \rightarrow A \rightarrow A' \rightarrow T' \rightarrow B' \rightarrow W$.

Также необходимо учесть, что у сотрудника есть право на обед или «перекур», моделирование чего представлено на Рисунке 2 – сценарий 2.

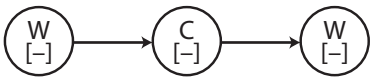

Рис. 2. Пример моделирования не директивных, но правомерных действий сотрудника (не регламентированных инструкцией по работе с документами)

Аналитически такие переходы между состояниями могут быть записаны следующим образом:

Сценарий 2: $W \rightarrow C \rightarrow W$,

где C – нахождение сотрудника в помещении «C».

Так, согласно Рисунку 2, сотрудник в некоторый момент времени может посетить помещение «C», а затем вернуться обратно на рабочее место; при нормальном стечении обстоятельств, документ в эти моменты у него отсутствует.

Для корректного моделирования обоих сценариев, представленных на Рисунках 1 и 2 (путем их отображения в едином пространстве), учтем близость состояний «T'» к «C» (как метрику в этом пространстве) следующих показателей состояния: физическое расположение (т.к. помещение «C» находиться около траектории от «A» к «B») и удовлетворенность потребностей (т.к. помещении «C» может обеспечить сотрудника едой или реализацией иных естественных потребностей и привычек). Аналитическая запись такой близости может быть записана следующим образом:

$$|P_1 - P_2| < \delta,$$

где P_1 и P_2 – некоторые состояния, «$|\ldots|$» – метрика или расстояние между состояниями в пространстве их показателей, δ – параметр близости состояний. Суть данной записи означает, что состояния называются близкими, если расстояние между ними меньше некоторого значения.

Моделирование обоих сценариев поведения сотрудника с учетом близости состояний приведено на Рисунке 3 (т.е. сценарии 1 и 2); пунктирными линиями показаны переходы между состояниями согласно предыдущим сценариям, а линиями с красными цифрами – возможное развитие событий.

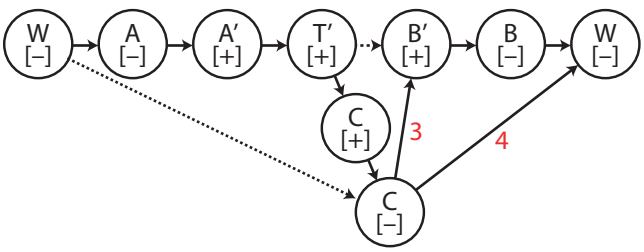

Рис. 3. Пример моделирования «мультисценарных» действий сотрудника

Так, следуя Рисунку 3, до состояния «T'» происходит корректное выполнение инструкции, за которым по причине близости состояний «T'» и «C» происходит «халатный переход» сотрудника во второе состояние, при этом при наличии на руках документа – «$C[+]$»; таким образом возникает первая предпосылка к неумышленному инсайдингу. Затем, по мере нахождения в помещении «С» и уже следуя его «правилам», сотрудник оказывается в состоянии «$C[-]$» – например, оставив документ на столе или полке. После этого можно предположить развитие действий сотрудника по двум вариациями совместного сценария: сценарий 3 – продолжающему выполнение текущего сценария 1, при котором сотрудник продолжит перемещение в пункт «В», перейдя для этого в состояние «B'» (модель которого приведена на Рисунке 1); сценарий 4 – срабатывание привычки сотрудника идти после помещения «С» на рабочее место, т.е. в состояние «W» (модель которого приведена на Рисунке 1). Такие сценарные развития показаны на Рисунке 3 красными цифрами.

Аналитически такие переходы между состояниями могут быть записаны следующим образом:

$$\begin{cases} \text{Сценарий 3: } W \to A \to A' \to T' \to C \to C \to B' \to W \\ \text{Сценарий 4: } W \to A \to A' \to T' \to C \to C \to W) \end{cases}$$

Достаточно показательным будет оценка изменения безопасности документа для всех вариантов развития действий сотрудника – двух сценариев и вариаций их объединения. Для этого условно можно считать, что при хранении документа в пунктах «А» и «В» его безопасность максимальна, при нахождении в руках сотрудника – средняя, а при оставлении документа сотрудником в общественном месте – минимальная. График такого изменения безопасности документа приведен на Рисунке 4.

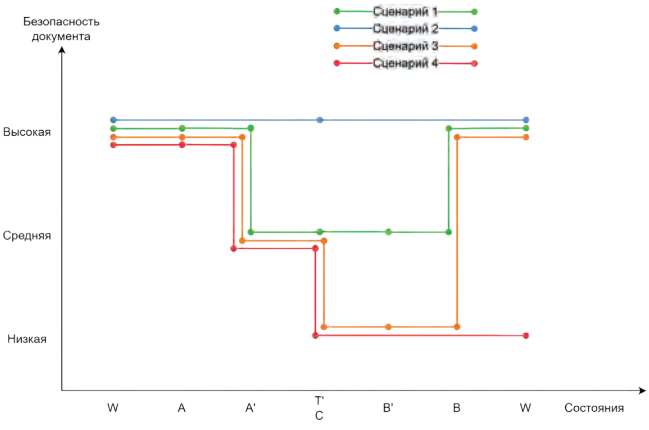

Рис.4. Безопасность документа при выполнении сотрудником действий по различным сценариям

Дадим интерпретацию предложенной динамике изменения безопасности документа, формализовав ее следующем образом:

$$S \in \{High = 3, Middle = 2, Low = 1\},$$

где S – (*аббр. от англ.* Security или Safety, *перев. на русс.* Безопасность) безопасность документа в некоторый момент времени, которая может следующего уровня (с числовыми значениями в скобках): High (*перев. с англ. на русс.* Высокая), Middle (Средняя) и Low (Низкая).

Исходя из того, что между состояниями сотрудника безопасность документа практически не меняется, то средняя оценка может быть произведена как суммирование ее значения на время перехода между состояниями, поделенное на общее время сценария, т.е.:

$$S = \frac{\sum_{i=1 \dots M-1} S_i \times T_i}{\sum_{i=1 \dots M-1} T_i},$$

где i – индекс состояния, M – количество всех состояний, S_i – безопасность документа в состоянии P_i, T_i – время нахождения сотрудника в i-м состоянии.

Для упрощения дальнейших расчетов (но без потери смысла) примем, что время перехода между состояниями одинаковое и равно t; в этом случае, суммарное время всех сценариев (даже с учетом 2-го, в котором не участвует документы) будем считать равным времени 1-го сценария, т.е. 6t.

В сценарии 1 до состояния «A'» и после состояния «B'» документ находится в хранилище и имеет высокую безопасность. В момент перенесения его сотрудником из пункта «А» в «В» безопасность снижается до средней, поскольку документ все также находится под контролем. В этом случае, безопасность такого сценария (с учетом ее числовых значений) равняется:

$$S\,(\text{Сценарий 1}) = \frac{3+3+2+2+2+3}{6} = 2{,}5.$$

В сценарии 2 документ продолжает находиться в хранилище все время и, следовательно, его безопасность не снижается, а безопасность равняется:

$$S\,(\text{Сценарий 2}) = \frac{3+3+3+3+3+3}{6} = 3.$$

В сценарии 3 вначале безопасность изменяется так же, как и в сценарии 1, однако в момент оставления сотрудником помещения «С» без документа, безопасность последнего снижается до низкой (поскольку он становится доступным третьим лицам) и продолжает такой оставаться на всем действии сценария. Безопасность документа в данном случае равняется:

$$S\,(\text{Сценарий 3}) = \frac{3+3+2+1+1+3}{6} \approx 2{,}33.$$

В сценарии 4, в отличие от 3, сотрудник после помещения «С» приходит в пункт «В», где выявляется факт потери документа, за которым, очевидно, следует введение нештатной ситуации с «изъятием» документа из помещения «С» в хранилище, где безопасность документа снова становится высокой. Таким образом, безопасность равняется:

$$S(\text{Сценарий } 4) = \frac{3+3+2+1+1+1}{6} \approx 1{,}83.$$

Как показало моделирование сценариев (и, в частности, неумышленного инсайдинга в сценариях 3 и 4), безопасность защищаемых документов имеет сложный (нелинейный) характер зависимости от динамики изменения состояний.

Этап 2. Метод синтеза

Несмотря на то, что предложенная Модель в принципе содержит всю необходимую информацию о поведении сотрудника в отношении защищаемых ИР согласно инструкции и иных действий в условиях организации, тем не менее, ее адекватное построение считается отдельно стоящей наукоемкой задачей структурно-параметрического синтеза. Также, проведение оценок безопасности ИР в процессе моделирования поведения сотрудников (и в особенности, при неумышленном инсайдинге) нуждается в создании соответствующего математического аппарата (ввиду отсутствия такового). В интересах этого необходимо создание специального Метода, гипотетическими фазами и шагами которого могут стать следующие.

Фаза 1. *Построение Модели*. Данная фаза предназначена для синтеза модели в аналитическом виде.

Шаг 1.1. *Сбор информации об организации*. На этом шаге необходимо собрать информацию о состояниях, которые может «посещать» сотрудник (конкретных или абстрактных в виде их группы), исходя из специфики организации (помещения, ИР, средства защиты, точки доступа и пр.).

Шаг 1.2. *Сбор информации о сотрудниках*. На этом шаге необходимо выделить основные факторы, влияющие на поведение (а точнее, на его девиацию) сотрудников, в том числе, с учетом специфики организации (например, потребность в отдыхе из-за сверхнапряженной эмоциональной работы).

Шаг 1.3. *Сбор информации об инструкциях*. На этом шаге необходимо из инструкций, которые требуется проверить на устойчивость, выделить состояния для сотрудника (например, пункты перемещение, хранилища документов, рабочие места, средства защиты и пр.).

Шаг 1.4. *Сбор информации о нерегламентированных действиях*. На этом шаге необходимо определить действия, которые может выполнять сотрудник, но которые не регламентируются инструкциями. Анализ таких сценариев позволит выделить состояния, возможные при девиации поведения сотрудников, поскольку они отражают не заранее заданные требования к поведению, а особенности человека.

Шаг 1.5. *Сбор информации о защищаемых ИР*. На этом шаге необходимо выделить защищаемые в организации ИР, а также влияние на них действий и состояний сотрудника (например, «грифованные» документы, ключи доступа и пр.)

Шаг 1.6. *Систематизация собранной информации*. На этом шаге необходимо систематизировать (а также и гармонизировать) всю собранную информацию, установив все необходимые связи (например, определить влияние внутренних факторов сотрудников на выполнение действий).

Шаг 1.7. *Формализация модели*. На этом шаге необходимо перевести всю собранную и систематизированную информацию в формализованный вид с использованием структуры и параметров Модели.

Фаза 2. *Моделирование поведения сотрудника*. Данная фаза предназначена для имитации поведения сотрудников в процессе выполнения инструкций с учетом близости состояний и возможности возникновения неумышленного инсайдинга; она состоит из следующих шагов. Также, в результате будет дана оценка устойчивости инструкции в контексте безопасности ИР.

Шаг 2.1. *Выбор должностной инструкции*. На этом шаге необходимо выбрать инструкцию, устойчивость которой требуется проверить, при этом, настроив необходимые для нее параметры с учетом специфики информации, собранной в Фазе 1 (например, как в примере, перемещение конфиденциального документа между двумя пунктами с указанием возможного маршрута и времени доставки).

Шаг 2.2. *Имитация действий сотрудника*. На этом шаге осуществляется непосредственное моделирование действий сотрудников в процессе выполнения инструкции путем имитации его передвижения по состояниями. При этом должны учитываться внутренние факторы сотрудника, пытающиеся «сбить» его с заданного маршрута (например, переход в близкое состояние из-за потребности в отдыхе). Сами факторы могут как задаваться постоянными величинами (например, сотрудники, как правило, с вероятностью 1% могут «заглянуть» в помещение для отдыха), так и учитывать специфику конкретного сотрудника, полученную на основании личностных и иных тестов (например, данный сотрудник, имея низкую потребность в отдыхе, тем не менее, обладает вредными привычками, которые соответствующим образом вносят девиацию в его поведение).

Шаг 2.3. *Оценка устойчивости инструкции*. На этом шаге на основании имитации действий сотрудника следует оценить устойчивость инструкции от изменения своего сценария через близкие состояния (например, как в примере, вероятность оставления документа в помещении С).

Шаг 2.4. *Оценка безопасности ИР при выполнении инструкции*. На этом шаге на основании имитации действий сотрудника следует оценить безопасность защищаемых ИР (усредненное значение или в динамике), исходя из возможных переходов сотрудника на близкие состояния и изменения сценария действий (например, как в примере, оценка средней S).

DOI: 10.21681/2311-3456-2024-6-108-116

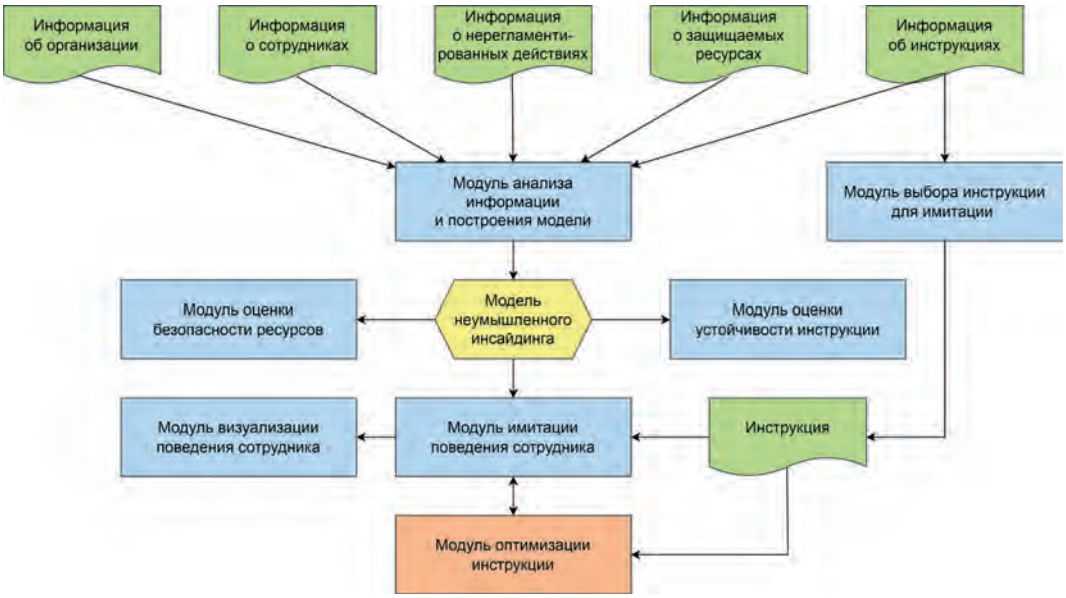

Рис. 5. Базовый структурный слой архитектуры Комплекса

Фаза 3. *Исправление инструкций*. Данная фаза предназначена для непосредственной корректировки инструкций, имеющих недостаточную устойчивость, что приводит к угрозе безопасности ИР.

Шаг 1. *Проверка результатов оценки инструкции*. На этом шаге специалист проверяет полученные оценки инструкции и, в случае удовлетворительного результата, оканчивает метод (например, если инструкция оказалась устойчивой). В противном случае – переход к Шагу 1'.

Шаг 1'. *Выявление «слабых» мест в инструкции*. На этом шаге специалист экспертно выявляет места в инструкции (состояния, переходы между ними, действия сотрудников и т.п.), приводящие к снижению ее устойчивости и потенциальному нарушению безопасности (собственно, слабые места будут являться, как правило, состояниями, из которых может происходить переход в смежные).

Шаг 2. *Корректировка «слабых» мест в инструкции*. На этом шаге специалист также экспертно вносит изменения в инструкцию, предполагая, что это приведет к ее улучшению – повышению устойчивости (например, меняет порядок действий, траекторию движения сотрудника или добавляет переходы через дополнительные состояния).

Шаг 3. *Повторная проверка инструкций*. Шаг является формальным и приводит к повторному переходу на Фазу 2 Метода, но уже с исправленной инструкцией. Таким образом, специалист получает возможность ручной «оптимизации» инструкции.

Следует отметить, что Фаза 3 может быть частично автоматизирована применением определенных техник оптимизации, поскольку в данном случае как устойчивость инструкций, так и безопасность ИР организации можно считать целевой функцией, требующей максимизации[3].

Этап 3. Программный комплекс

Для автоматизации Метода может быть применена область программной инженерии, так как потребуется создать программный комплекс для моделирования инструкций на основании собранной специалистом информации (далее – Комплекс). Такое программное решение позволит, как визуально имитировать деятельность сотрудников, так и автоматически производить необходимые вычисления (устойчивости инструкций и безопасности ИР). Интерактивность работы с Комплексом даст возможность специалисту корректировать инструкции и оценивать получаемые результаты.

Базовый структурный слой архитектуры Комплекса (как совокупности логических модулей и их связей) может иметь вид, представленный на Рисунке 5.

Структурный слой архитектуры (см. Рисунок 5) является интуитивно понятным и полностью отражает работу Метода, функционирующего на основании Модели. Архитектурными элементами Комплекса являются следующие:

1. «Информация об организации» – вводимая информация, собираемая на Шаге 1.1 Метода (далее – на Шаге);
2. «Информация о сотрудниках» – вводимая информация, собираемая на Шаге 1.2;
3. «Информация о нерегламентированных действиях» – вводимая информация, собираемая на Шаге 1.4;

3 Смоленцева Т. Е. Методы определения целевой функции организационных систем // Моделирование, оптимизация и информационные технологии. 2018. Т. 6. № 3 (22). С. 143–152.

4. «Информация о защищаемых ресурсах» – вводимая информация, собираемая на Шаге 1.5;
5. «Информация об инструкциях» – вводимая информация, собираемая на Шаге 1.3;
6. «Модуль анализа информации и построения модели» – модуль для формализации вводимой информации с целью построения Модели;
7. «Модель неумышленного инсайдинга» – формализованное представление Модели, готовой для имитационного моделирования и проведения оценок;
8. «Модуль выбора инструкции для имитации» – модуль для взаимодействия с оператором в интересах выбора инструкции, необходимой для моделирования;
9. «Инструкция» – формализованное представление инструкции, подходящее для проведения моделирования (в т.ч. в процессе оптимизации);
10. «Модуль имитации поведения сотрудника» – основной модуль Комплекса, позволяющий проводить моделирование действий сотрудника с учетом возникновения инцидентов неумышленного инсайдинга (т.е. переходов на близкие состояния);
11. «Модуль визуализации поведения сотрудника» – модуль для отображения оператору процесса деятельности сотрудника согласно заданной инструкции в графическом или текстовом виде;
12. «Модуль оценки безопасности ресурсов» – модуль для вычислений различных метрик, связанных с безопасностью ИР в соответствии с текущей моделируемой инструкцией;
13. «Модуль оценки устойчивости инструкции» – модуль для вычислений различных метрик, связанных с устойчивостью текущей моделируемой инструкции;
14. «Модуль оптимизации инструкции» – гипотетический модуль, упомянутый при описании метода, проводящий оптимизацию инструкции путем ее структурно-параметрических изменений и оценки влияния этого на целевые функции (вычисляемые модулями под номерами 12 и 13).

Данный комплекс, в случае успешной реализации, предоставит достаточно мощный инструмент как для моделирования, так и оценки выполнения сотрудником инструкций с позиции их устойчивости, а также безопасности ИР организации.

Заключение

Работа посвящена противодействию неумышленному инсайдингу, ведущему к нарушениям информационной безопасности в организациях и качественно отличного от других видов угроз тем, что он сложно выявляем на ранних этапах (например, тестирование сотрудников) и имеет вполне легальный источник (поскольку угроза может исходить от добропорядочных сотрудников). Поскольку данная «застаревшая» проблема в принципе является достаточно «свежей» для науки (то есть, слабо освещенной в научных публикациях), то предлагается проведение отдельного, целостного научного исследования по канонической схеме с созданием таких научных результатов, как аналитическая модель предметной области, метод синтеза устойчивых регламентов деятельности и архитектура программного комплекса моделирования инструкций (естественно, с последующей его реализацией и оценкой). Гипотетически это позволит получить новые научные результаты, на данный момент не имеющие релевантных аналогов.

Новизна работы состоит в том, что впервые в качестве уязвимости организации рассматривается «неустойчивость» регламентов деятельности сотрудников (инструкции), а в качестве источника угрозы безопасности ИР – девиация поведения сотрудников, вследствие чего происходит отклонение от шагов инструкции.

Теоретическая значимость работы состоит в переводе деятельности, традиционно описываемой на естественном языке, в аналитическую плоскость. Практическая же значимость определяется применением каждого из результатов для повышения безопасности защищаемых ИР в практически любой организации, связанной с ИТ.

В контексте последней «связки», продолжением исследования должна стать глубокая научная проработка вопросов проецирования соответствующих результатов на сферу ИТ, то есть на виртуальную (цифровую) среду деятельности неумышленного инсайдера по отношению к ИР организации.

Литература

1. *Buinevich M., Izrailov K., Kotenko I., Ushakov I., Vlasov D. Approach to combining different methods for detecting insiders // The proceedings of 4th International Conference on Future Networks and Distributed Systems (New York, USA, 2020). Iss. 26. PP. 1–6. DOI: 10.1145/3440749.3442619.*
2. *Власов Д. С. К вопросу о мотивации инсайдера организации и способах его классификации // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2022. № 1. С. 128–147.*
3. *Власов Д. С. Мультикритериальная модель систематизации способов обнаружения инсайдера // Вопросы кибербезопасности. 2024. № 2 (60). С. 66–73. DOI: 10.21681/2311-3456-2024-2-66-73.*
4. *Буйневич М. В., Власов Д. С., Моисеенко Г. Ю. Комбинирование способов выявления инсайдеров больших информационных систем // Вопросы кибербезопасности. 2024. № 3 (61). С. 2–13. DOI: 10.21681/2311-3456-2024-3-2-13.*
5. *Анализ и систематизация инсайдерских угроз в информационных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021): сборник научных статей (Санкт-Петербург, 24–25 февраля 2021 года). Т. 4. 2021. С. 399–403*

6. Буйневич М. В., Власов Д. С. Сравнительный обзор способов выявления инсайдеров в информационных системах // Информатизация и связь. 2019. № 2. С. 83–91. DOI: 10.34219/2078-8320-2019-10-2-83-91.
7. Васильев М. В., Федорова А. В. Несоответствие должностных инструкций сотрудников банковской сферы новым угрозам информационной безопасности // Поколение будущего: Взгляд молодых ученых- 2019: сборник научных статей 8-й Международной молодежной научной конференции (Курск, 13–14 ноября 2019 года). 2019. С. 253–255.
8. Нашивочников Н. В. Выявление отклонений в поведенческих паттернах пользователей корпоративных информационных ресурсов с использованием топологических признаков // Вопросы кибербезопасности. 2023. № 4 (56). С. 12–22. DOI: 10.21681/2311-3456-2023-4-12-22.
9. Поляничко М. А. Методика обнаружения аномального взаимодействия пользователей с информационными активами для выявления инсайдерской деятельности // Труды учебных заведений связи. 2020. Т. 6. № 1. С. 94-98. DOI: 10.31854/1813-324X-2020-6-1-94-98.
10. Астахова Л. В. Модель нулевого доверия как фактор влияния на информационное поведение сотрудников организации // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2022. № 3. С. 13–17. DOI: 10.36535/0548-0019-2022-03-2.

THE INSTRUCTIONS «RESISTANT» INCREASING AS A WAY TO COUNTER UNINTENTIONAL INSIDING

Buinevich M. V.[4], Moiseenko G. Yu.[5]

The goal of the investigation: *ensuring the organization's information resources security from threat of unintentional including by increasing instructions «resistant».*

Research methods: *systems analysis, analytical modeling, synthesis, hypothetical experiment, software engineering.*

Results: *a graphoanalytical model of the unintentional insiding are obtained, a step-by-step method for synthesizing resistant instructions and the architecture of a software package for they modeling are developed. It is assumed that these scientific results currently have no relevant analogues. The theoretical significance of the work consists in translating the activities traditionally described in natural language into an analytical plane. The practical significance is determined by the application of each of the results to improve the protected information resources security in almost any organization related to information technology.*

The scientific novelty *lies in the fact that for the first time, the «instability» of employee regulations is considered as an organization's vulnerability; the employee behaviors deviation is considered as to the security of information resources threat source, as a result of which there is a deviation from the instructions steps.*

Keywords: *information resources, instructions, unintentional insiding, security threat, counteraction method, modeling.*

References

1. Buinevich M., Izrailov K., Kotenko I., Ushakov I., Vlasov D. Approach to combining different methods for detecting insiders // The proceedings of 4th International Conference on Future Networks and Distributed Sys-tems (New York, USA, 2020). Iss. 26. PP. 1–6. DOI: 10.1145/3440749.3442619.
2. Vlasov D. S. K voprosu o motivatsii insaydera organizatsii i sposobakh yego klassifikatsii // Elek-tronnyy setevoy politematicheskiy zhurnal «Nauchnyye trudy KubGTU». 2022. № 1. S. 128–147.
3. Vlasov D. S. Mul'tikriterial'naya model' sistematizatsii sposobov obnaruzheniya insaydera // Vo-prosy kiberbezopasnosti. 2024. № 2 (60). S. 66–73. DOI: 10.21681/2311-3456-2024-2-66-73.
4. Buynevich M. V., Vlasov D. S., Moiseyenko G. YU. Kombinirovaniye sposobov vyyavleniya insayderov bol'shikh informatsionnykh sistem // Voprosy kiberbezopasnosti. 2024. № 3 (61). S. 2–13. DOI: 10.21681/2311-3456-2024-3-2-13.
5. Analiz i sistematizatsiya insayderskikh ugroz v informatsionnykh sistemakh // Aktual'nyye problemy infotelekommunikatsiy v nauke i obrazovanii (APINO 2021): sbornik nauchnykh statey (Sankt-Peterburg, 24–25 fevralya 2021 goda). T. 4. 2021. S. 399–403.
6. Buynevich M. V., Vlasov D. S. Sravnitel'nyy obzor sposobov vyyavleniya insayderov v informatsi-onnykh sistemakh // Informatizatsiya i svyaz'. 2019. № 2. S. 83–91. DOI: 10.34219/2078-8320-2019-10-2-83-91.
7. Vasil'yev M. V., Fedorova A. V. Nesootvetstviye dolzhnostnykh instruktsiy sotrudnikov bankovskoy sfery novym ugrozam informatsionnoy bezopasnosti // Pokoleniye budushchego: Vzglyad molodykh uchenykh- 2019: sbornik nauchnykh statey 8-y Mezhdunarodnoy molodezhnoy nauchnoy konferentsii (Kursk, 13–14 noyabrya 2019 goda). 2019. S. 253–255.
8. Nashivochnikov N. V. Vyyavleniye otkloneniy v povedencheskikh patternakh pol'zovateley korporativ-nykh informatsionnykh resursov s ispol'zovaniyem topologicheskikh priznakov // Voprosy kiberbezopasnosti. 2023. № 4 (56). S. 12-22. DOI: 10.21681/2311-3456-2023-4-12-22.
9. Polyanichko M. A. Metodika obnaruzheniya anomal'nogo vzaimodeystviya pol'zovateley s informatsi-onnymi aktivami dlya vyyavleniya insayderskoy deyatel'nosti // Trudy uchebnykh zavedeniy svyazi. 2020. T. 6. № 1. S. 94-98. DOI: 10.31854/1813-324X-2020-6-1-94-98.
10. Astakhova L. V. Model' nulevogo doveriya kak faktor vliyaniya na informatsionnoye povedeniye sotrud-nikov organizatsii // Nauchno-tekhnicheskaya informatsiya. Seriya 1: Organizatsiya i metodika informatsionnoy raboty. 2022. № 3. S. 13-17. DOI: 10.36535/0548-0019-2022-03-2

4 Mikhail V. Buinevich, Dr.Sc., Professor, Professor of Dep. Applied Mathematics and Information Technologies of Saint-Petersburg University of State Fire Service of EMERCOM of Russia, Saint-Petersburg, Russia. ORCHID: https://orcid.org/0000-0001-8146-0022. Scopus Author ID: 56122749800. E-mail: bmv1958@yandex.ru
5 Grigory Yu. Moiseenko, Head of direction, Ministry of Defense of the Russian Federation, Moscow, Russia. E-mail: mogreq@mail.ru