Функционально-системный подход к управлению информационной безопасностью

En **A Possible Approach to the Information Security Assessment**

V. V. Bondarev,
PhD (Mil.), Associated Professor
BMSTU, Training center «Informzaschita»
bondarevvv@mail.ru

Essence of concepts «Management by informative safety» and «control system open up informative safety». The different going is examined near a management by informative safety of organization. The review of existent measures of counteraction to the threats of informative safety, nocifensors and principles of providing/of management informative safety is given. Difficulties impedimental to the decision of tasks of analysis and synthesis of control system by informative safety are analysed. Offer new decision of management problem by informative safety on on the basis of the use functional-approach of the systems.

Keywords: information security, control system, automated system, security, analysis, synthesis, information technologies

Раскрывается сущность понятий «управление информационной безопасностью» и «система управления информационной безопасностью». Рассматриваются различные подходы к управлению ИБ организации. Дается обзор существующих мер противодействия угрозам ИБ, защитных механизмов и принципов обеспечения/управления ИБ. Проанализированы трудности, препятствующие решению задач анализа и синтеза систем управления ИБ. Предложено новое решение проблемы управления ИБ на основе использования функционально-системного подхода.

Ключевые слова: информационная безопасность, система управления, автоматизированная система, безопасность, анализ, синтез, информационные технологии

Валерий Васильевич Бондарев,
кандидат военных наук, доцент
МГТУ им. Н. Э. Баумана,
преподаватель АНО ДПО
«Учебный центр «Информзащита»
bondarevvv@mail.ru

Существует несколько подходов к построению систем управления ИБ (СУИБ) организации. Например, нормативный подход (защита гостайны), процессный подход (серия стандартов ISO 27x) и др. Можно многое сказать и о недостатках, и о достоинствах этих подходов. Однако в данной статье сделана попытка предложить принципиально новую концепцию построения СУИБ – на основании функционально-системного подхода, которая, по мнению автора, может интегрировать достоинства и нивелировать недостатки уже существующих подходов.

Но сначала давайте вспомним общеизвестные истины.

Управление информационной безопасностью (*Security information management*, SIM) – это циклический процесс, включающий:

- осознание степени необходимости защиты информации и постановку задач;
- сбор и анализ данных о состоянии информационной безопасности в организации;
- оценку информационных рисков;
- планирование мер по обработке рисков;
- реализацию и внедрение соответствующих механизмов контроля, распределение ролей и ответственности, обучение и мотивацию персонала, оперативную работу по осуществлению защитных мероприятий;
- мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие воздействия [1].

Согласно ISO 27001, СУИБ – это «та часть общей системы управления организации, основанной на оценке бизнес-рисков, которая создает, реализует, эксплуатирует, осуществляет мониторинг, пересмотр, сопровождение и совершенствование информационной безопасности». Система

управления включает в себя организационную структуру, политики, планирование, должностные обязанности, практики, процедуры, процессы и ресурсы.

При рассмотрении проблемы управления информационной безопасностью (ИБ) следует всегда исходить из того, что защита информации и самой системы ее обработки не является самоцелью.

Конечной целью обеспечения безопасности автоматизированной системы (АС) является защита всех категорий субъектов (как внешних, так и внутренних), прямо или косвенно участвующих в процессах информационного взаимодействия, от нанесения им ощутимого материального, морального или иного ущерба в результате случайных или преднамеренных нежелательных воздействий на информацию и системы ее обработки и передачи. В качестве защищаемых объектов должны рассматриваться информация, все ее носители (отдельные компоненты и автоматизированная система обработки информации в целом) и процессы обработки.

Целью защиты циркулирующей в АС информации является предотвращение ее разглашения (утечки), искажения (модификации), утраты, блокирования (снижения степени доступности) или незаконного тиражирования.

Обеспечение безопасности АС предполагает создание препятствий для любого несанкционированного вмешательства в процесс ее функционирования, а также для попыток хищения, модификации, выведения из строя или разрушения ее компонентов, то есть защиту всех компонентов АС: оборудования, программного обеспечения, данных (информации) и персонала.

Меры противодействия угрозам ИБ можно классифицировать следующим образом.

Правовые – действующие в стране законы, указы и другие нормативные правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее получения, обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации, и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом АС.

Морально-этические – нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как требования нормативных актов, однако их несоблюдение обычно ведет к падению авторитета или престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т. п.), так и писаные, то есть оформленные в некоторый свод (устав, кодекс чести и т. п.) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах пользователей и обслуживающего персонала АС).

Организационные – меры административного и процедурного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей и обслуживающего персонала с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Технологические – разного рода технологические решения и приемы, основанные обычно на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т. п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий. Примером таких мер является использование процедур двойного ввода ответственной информации, инициализация ответственных операций только при наличии разрешений от нескольких должностных лиц, процедуры проверки соответствия реквизитов исходящих и входящих сообщений в системах коммутации сообщений, периодическое подведение общего баланса всех банковских счетов и т. п.

Физические – основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также средств визуального наблюдения, связи и охранной сигнализации. К данному типу относятся также меры и средства контроля физической целостности компонентов АС (пломбы, наклейки и т. п.

Программно-технические – основаны на использовании различных электронных устройств и специальных программ, входящих в состав АС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты.

Все перечисленные виды и меры обеспечения ИБ лежат в основе следующих защитных механизмов, предназначенных для защиты АС от неправомерного вмешательства в процессы их функционирования и НСД к информации:

- идентификация (именование и опознавание), аутентификация (подтверждение подлинности) пользователей системы;
- разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий пользователям);
- регистрация и оперативное оповещение о событиях, происходящих в системе;
- криптографическое закрытие (шифрование) данных, хранимых и передаваемых по каналам связи;
- контроль целостности и аутентичности (подлинности и авторства) данных;

- резервирование и резервное копирование;
- фильтрация трафика и трансляция адресов;
- обнаружение вторжений (атак);
- выявление и нейтрализация действий компьютерных вирусов;
- затирание остаточной информации на носителях;
- выявление уязвимостей (слабых мест) системы;
- маскировка и создание ложных объектов;
- страхование информационных рисков.

Однако классификация механизмов защиты может быть и другой.

Перечисленные механизмы защиты объединяются в систему управления ИБ, могут применяться в конкретных технических средствах и системах защиты в различных комбинациях и вариациях.

Построение системы управлением ИБ должно основываться на определенных принципах, таких как:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- разумная достаточность;
- персональная ответственность;
- разделение функций;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- взаимодействие и координация;
- обязательность контроля (перечень не полный).

Среди перечисленных принципов к наиболее труднореализуемым по тем или иным причинам относится принцип ***комплексности*** (согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов) и ***системности*** (учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации в АС).

Поскольку обеспечение безопасности информационных технологий есть процесс управления рисками, то система защиты – это система управления, реализующая технологию обеспечения безопасности (управления ИБ). Любая технология предусматривает определенный набор операций и процессов взаимодействия их исполнителей, направленный на достижение конечного результата (цели).

Цель – достижение заданного (приемлемого) уровня ИБ организации (предприятия). Предполагает распределение функций между исполнителями и организацию процессов их взаимодействия. Необходима согласованность (координация) действий и реальная выполнимость функций всеми исполнителями.

Система управления ИБ организации является сложной организационно-технической системой. При исследовании систем вообще и систем управления в частности применяют методы анализа (изучение свойств и поведения в зависимости от структуры и характеристик) и синтеза (выбор структуры и характеристик исходя из заданных свойств). Изучение таких систем путем прямых экспериментов невозможно, а их частей, вследствие эмерджентности, – бесполезно.

Анализ. Построение математической модели системы на ЭВМ возможно в случае, если реальные процессы в большой системе являются марковскими, то есть когда определенные числовые параметры, характеризующие процесс в данный момент, достаточны для перехода к следующему этапу.

Рассмотрим модель системы в общем виде (рис. 1), где $X(t)$ – входная функция, $Y(t)$ – выходная функция, $q(t)$ – состояние системы. При фиксированной входной функции $X(t)$ имеем случайную выходную функцию $Y(t)$. Строится вероятное соотношение между входной и выходной функциями при фиксированном состоянии. Каждой входной функции $X(t)$ сопоставляется вероятная мера $Lx(Y)$ на множестве допустимых выходных функций $Y(t)$. Это и есть функция системы.

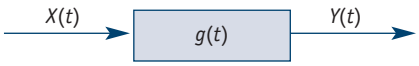

Рис. 1. ***Модель системы в общем виде***

Как отмечает известный физиолог П. К. Анохин, «в результате многолетней практики такого подхода ни одна из тысяч математических моделей нейрона абсолютно не отразила истинные особенности нейрона и ни на один шаг не продвинулись вперед наши знания о действительных законах его функционирования» [2].

Одна из главных причин неудач заключается в использовании понятия «взаимодействие». Может ли взаимодействие компонентов создать что-то системное?

Пример Эшби [3] подтверждает мысль о невозможности этого. Взаимодействие ведет лишь к хаосу, а не к организованному поведению организма.

Определение системы, базируясь на связях, взаимодействии, не позволяет моделировать и изучать системы. Нужно вскрыть некоторые детерминирующие факторы, имеющиеся в реальных живых системах, освобождающие компоненты системы от избыточных степеней свободы. Формулировка «упорядоченное множество» не позволяет избежать «проклятия размерности», вызывая дополнительный вопрос: кто и по какому критерию упорядочивает?

Синтез. Пусть имеется k типов сложных систем, из которых можно построить большую систему.

В случае если система состоит из n_1 устройств 1-го типа, n_2 – 2-го типа, n_k – k-го типа, то ее можно характеризовать вектором

$$\overline{n} = (n_1, n_2, \ldots, n_k).$$

Задаваясь множеством N допустимых векторов , строятся только те системы, которые характеризуются вектором $\overline{n} \in N$.

Пусть в пространстве точек вида $L_x(y)$ задано множество R точек этого пространства. Цель синтеза – построение такой системы, для которой $L_x(y) \in R$, $\overline{n} \in N$. Вводя в множество N операцию упорядочивания, то есть функцию предпочтительности $W(n)$ (из двух факторов n_1, n_2, один предпочтительнее другого), получают оптимальный синтез, когда $W(n) = min$.

Методы формального решения задач синтеза имеются лишь для случая конечных автоматов.

С учетом изложенных выше трудностей в исследовании систем управления, в том числе систем управления ИБ, целесообразно обратить внимание на методы моделирования систем живых организмов в физиологии и психологии, в частности, на представление функциональной системы.

Модель большой системы (функциональной системы П. К. Анохина) строится на следующих свойствах, присущих системе, а не ее компонентам.

1. Ни одна организация, сколь бы обширной она ни была по количеству составляющих ее компонентов, не может быть названа самоуправляемой, саморегулируемой, если ее функционирование, то есть взаимодействие частей этой организации, не заканчивается каким-либо полезным для организации результатом и если отсутствует обратная афферентация (понятие, аналогичное понятию «обратная связь» в современной кибернетике) в управляющий центр о степени полезности этого результата.

2. Полезный результат организует систему в пространстве и времени, а в случае недостаточного результата – реорганизует расположение частей системы в пространстве и времени для обеспечения нового результата.

П. К. Анохин сформулировал следующее определение системы: «Системой можно назвать только такой комплекс избирательно вовлеченных компонентов, у которых взаимодействие и взаимоотношения приобретают характер взаимосодействия на получение фокусированного полезного результата» [2].

Конкретным механизмом взаимосодействия компонентов является освобождение их от избыточных степеней свободы, не нужных для получения данного конкретного результата, и, наоборот, сохранение всех тех степеней свободы, которые способствуют получению результата (под степенью свободы понимаются различные способы функционирования элементов, различные виды соотношения их со средой [4]).

Результат является компонентом системы, инструментом, создающим упорядоченное взаимодействие между всеми другими компонентами.

Поскольку результат является функциональным феноменом, то и система, сформированная результатом, названа функциональной.

Параметры результата формируются системой (компонентом) в виде определенной модели (образа) раньше, чем появится сам результат. Результат как системообразующий фактор отбирает все адекватные для данного момента степени свободы компонентов системы и фокусирует их усилия на себе.

Функциональная система – организация многих компонентов, динамически мобилизуемых в масштабах целого организма, системы. Компоненты той или иной структурной принадлежности мобилизуются и вовлекаются в функциональную систему только в меру их содействия получению запланированного результата.

Под свойством мобильности понимается способность моментального построения любых комбинаций компонентов для получения полезного результата.

Главная черта каждой функциональной системы – ее динамичность, исключительная мобильность, позволяющая этой системе быть пластичной, быстро менять свою структуру в поисках запрограммированного полезного результата.

Определим состав системы и роль ее отдельных компонентов.

Внесение понятия структуры в формулировку системы привносит нечто детерминированное. Между тем, одним из самых характерных свойств функциональной системы является именно динамическая изменчивость входящих в нее структурных компонентов, продолжающаяся вплоть до получения соответствующего полезного результата.

Таким образом, существование результата как фактора образования системы и ее фазовых реорганизаций, а также наличие специфического строения структурных механизмов, дающего возможность немедленного объединения их в систему, говорит о том, что истинные системы организма всегда функциональны по своей сути. Это означает, что функциональный принцип выборочной мобилизации структур является доминирующим, вследствие чего такие системы и названы функциональными.

Все функциональные системы независимо от уровня организации и количества составляющих их компонентов имеют принципиально одну и ту же функциональную архитектуру, в которой результат является доминирующим фактором, стабилизирующим организацию системы. Отсюда следует: при образовании иерархии систем всякий более низкий уровень систем должен организовать контакт результатов, что и может составить более высокий уровень систем. Наоборот, более высокий уровень должен произвести декомпозицию результата всей системы на результаты подсистем.

Понятие функциональной системы, зародившись в физиологии для описания живых систем, использованное в психологии для описания психических процессов, не может быть однозначно использовано в других областях человеческой деятельности, в том числе и в управлении информационной безопасности.

С целью практического использования этого понятия не только для объяснения свойств живого организма и субъекта, но и для решения практических задач, связанных с созданием систем управления, их эксплуатацией и применением, необходимо создать язык, пригодный для описания этих систем, адекватный языку описания функциональных систем, более детально описать механизмы и результаты действия и т. д. Такие исследования были проведены и опубликованы в [5]. Результат

одного из них – система управления – приведен на рис. 2.

Краткое пояснение к приведенной на рисунке схеме.

R – рецепторы (чувствительные нервные окончания или специализированные клетки, воспринимающие раздражения из внешней или внутренней среды и преобразующие их в нервное возбуждение, передаваемое в виде потока нервных импульсов в центральную нервную систему организма);

E – эффекторы (органы или системы органов, реагирующие (посредством нейрогуморальных механизмов) на действие внешних или внутренних раздражителей и выступающие в роли исполнительного звена рефлекторного акта);

S – сенсор (чувствительное к какому-либо воздействию устройство или элемент, сигнал которого, вырабатываемый им в результате воздействия, используется в дальнейшем регистрирующей или информационно-измерительной системой);

П – память;

Р – компонент принятия решения;

М – компоненты моторики (под моторикой понимают последовательность движений, в своей совокупности необходимых для выполнения какой-либо определенной задачи);

Э – двигательные (моторные) волокна, передающие возбуждение от центральной нервной системы к рабочим органам.

Безусловно, все эти термины (эффекторы, сенсоры, моторика и пр.) необходимо заменить на соответствующие им из предметных областей «информационная безопасность», «теория управления» и т. д. Но главное, что ***алгоритм деятельности (действия) по управлению вообще и управлению информационной безопасностью в частности представляется в виде***:

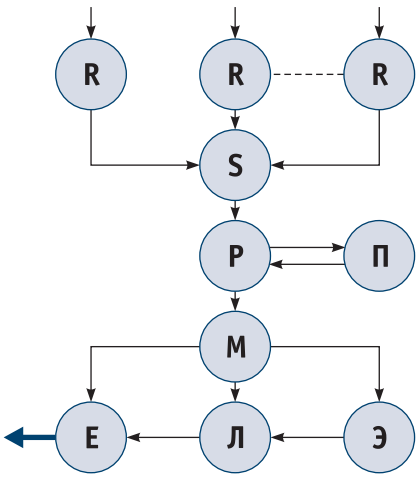

Рис. 2. ***Система управления***

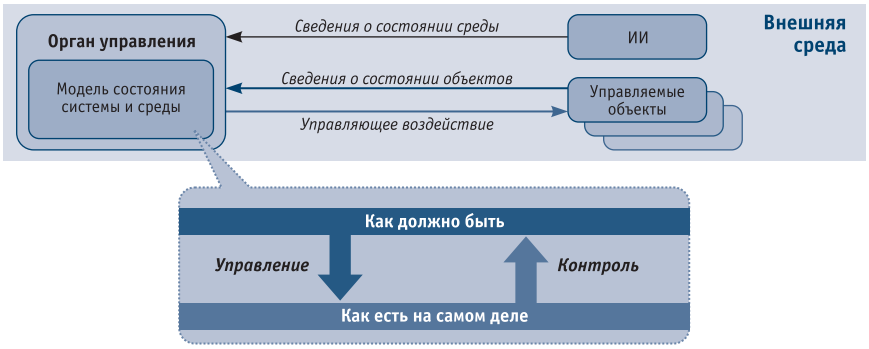

Рис. 3. ***Технология управления информационной безопасностью***

1) выявления проблемной ситуации (уяснение задачи – целеполагание, оценка обстановки – отображение ситуации);

2) мысленного выдвижения гипотез о путях достижения цели (с использованием образов ситуаций и действий из памяти определяются варианты достижения цели из текущей ситуации – выработка замысла на предстоящее действие);

3) оценки вариантов и выбора наилучшего по какому-либо критерию;

4) обеспечения достижения требуемого результата (формирование решения (программы, приказы), постановка задач исполнителям, обеспечение действий исполнителей, контроль достижения цели).

Анализируя изложенное выше, можно перейти к технологии управления ИБ, основываясь именно на функционально-системном подходе (рис. 3).

Орган/субъект управления (например, отдел технической защиты информации или Совет по управлению ИБ и т. п.) разрабатывает несколько моделей, как минимум, две. Одна – эталонная («как должно быть») – формируется на основе заранее разработанной политики безопасности. Вторая – текущая («как есть на самом деле») – на основе данных, полученных от системы мониторинга и от источников информации о состоянии внешней среды, например, законодательной. Смысл управления – в совмещении этих моделей. В процессе управления производится оценка эффективности (контроль). По результатам контроля корректируется вектор управляющих воздействий. В этой технологии результат – обеспечение приемлемого уровня безопасности – является компонентом системы управления ИБ. Вклад же отдельных механизмов защиты в достижение этого результата можно вычислить на основе коэффициента близости мер, изложенного в [6].

Таким образом, в настоящей публикации рассмотрена новая концепция построения СУИБ – на основании функционально-системного подхода. Более детальная проработка данного подхода будет приведена в последующих статьях. ■

ЛИТЕРАТУРА

1. GlobalTrust Solutions. Продукты и услуги в области информационной безопасности. Понятие системы управления информационной безопасностью [Электронный ресурс]. – Режим доступа: http://www.globaltrust.ru/ru/uslugi/vnedrenie-sistem-upravleniya-informacionnoi-bezopasnostyu/ponyatie-sistemy-upravleniya-informacionnoi-bezopasnostyu/.

2. Анохин П. К. Теория функциональной системы // Успехи физиологических наук. – 1970. – Т. 1, № 1. – С. 19–54.

3. Эшби У. Р. Введение в кибернетику. – М.: Иностранная литература. – 1959. – 432 с.

4. Ухтомский А. А. Доминанта. – СПб.: Питер. – 2002. – 448 с.

5. Колесников и др. Эргономическое обеспечение деятельности космонавтов. – М.: Машиностроение. – 1985. – 254 с.

6. Бондарев В. В. Возможный подход к оценке средств защиты информации // Защита информации. Инсайд. – 2017. – № 3 (75). – С. 76–78.