ЭКОНОМИКА

Макаров Александр Данилович
д-р юрид. наук, д-р экон. наук, профессор,
Заслуженный деятель науки и образования,
основатель научной школы РАЕ
ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»
г. Санкт-Петербург
Швед Виктор Григорьевич
д-р воен. наук, д-р техн. наук, профессор
НОУ ДПО «Учебный центр «СпецПроект»
г. Санкт-Петербург
Швед Дарья Викторовна
студентка
ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»
г. Санкт-Петербург

ИННОВАЦИОННЫЙ ПОДХОД В РОССИЙСКОЙ ЭКОНОМИКЕ – ФОРМАЛЬНАЯ МОДЕЛЬ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Аннотация*: в статье предлагается инновационный методический подход к реализации процесса подготовки и обоснования решений на основе анализа стандартных ситуаций, возникающих в деятельности руководителей организаций, службы информационной безопасности и структурных подразделений по защите информации.*

Ключевые слова*: безопасность, государство, достоверность, доступность, инновационность, инновационная деятельность, информационная безопасность, информационные ресурсы, конфиденциальность, целостность.*

В последнее пятилетие под информационной безопасностью государства понимают состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере. В современном социуме информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т.п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью[4]

Большая часть специалистов, работающих в сфере национальной, информационной безопасности в последнее время используют следующие понятия и определения, которые стандартизированы и унифицированы.

Информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности информации.

*Целостность. Целостность информаци*и (также целостность данных) – термин, большей частью используемый в информатике (криптографии, теории телекоммуникаций, теории информационной безопасности), означающий, что данные не были изменены при выполнении какой-либо операции над ними, будь то передача, хранение или отображение.

В телекоммуникации целостность данных часто проверяют, используя хеш-сумму сообщения, вычисленную алгоритмом MAC (от английского *message authentication code*). Значение хеш-суммы может использоваться для проверки целостности данных, их идентификации и поиска (например, в P2P-сетях), а также заменять собой данные, которые небезопасно хранить в явном виде (например, пароли, ответы на вопросы тестов и т.д.). Также алгоритмы хеширования используются для проверки целостности и подлинности файлов. Одноранговая, децентрализованная или пиринговая (от англ. *peer-to-peer,* P2P – равный к равному) сеть – это оверлейная компьютерная сеть, основанная на равноправии участников. Часто в такой сети отсутствуют выделенные серверы, а каждый узел

(*peer*) является как клиентом, так и выполняет функции сервера. В отличие от архитектуры клиент-сервера, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов. Участниками сети являются пиры.

В криптографии и информационной безопасности целостность данных (в широком смысле) – это сохранение данных в том виде, в каком они были созданы. Примеры нарушений целостности данных:

– попытка злоумышленника изменить номер аккаунта в банковской транзакции, или попытка подделки документа;

– случайное изменение информации при передаче или при неисправной работе винчестера (жесткого диска);

– искажение фактов СМИ (средствами массовой информации) с целью манипуляции общественным мнением.

В теории баз данных целостность данных означает корректность данных и их непротиворечивость. Обычно она также включает целостность связей, которая исключает ошибки связей между первичным и вторичным ключом. Примеры нарушений целостности данных:

– существование записей-сирот (дочерних записей, не имеющих связи с родительскими записями);

– существование одинаковых первичных ключей.

Для проверки целостности данных в криптографии используются хеш-функции, например, MD5. Хэш-функция преобразует последовательность байт произвольного размера в последовательность байт фиксированного размера (число). Если данные изменятся, то и число, генерируемое хеш-функцией, тоже изменится.

Целостность данных – свойство, при выполнении которого данные сохраняют заранее определённый вид и качество.

Доступность: обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Информационная безопасность (от англ. *information security*) – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчётности, аутентичности и достоверности информации или средств её обработки.

Безопасность информации (данных) (от англ. *information (data) security*) – состояние защищённости информации (данных), при котором обеспечиваются её (их) конфиденциальность, доступность и целостность.

Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе.

Безопасность информации (при применении информационных технологий) (от англ. *IT security*) – состояние защищённости информации (данных), обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована.

Безопасность автоматизированной информационной системы – состояние защищённости автоматизированной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчётность и подлинность её ресурсов.

Информационная безопасность – защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений. Поддерживающая инфраструктура – системы электро-, тепло-, водо-, газоснабжения, системы кондиционирования и т.д., а также обслуживающий персонал. Неприемлемый ущерб – ущерб, которым нельзя пренебречь[3]

Существенные признаки понятия

В качестве стандартной модели безопасности часто приводят модель из трёх категорий:

– конфиденциальность (от англ. *confidentiality*) – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на неё право;

– целостность (от англ. *integrity*) – избежание несанкционированной модификации информации;

– доступность (от англ. *availability*) – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Выделяют и другие не всегда обязательные категории модели безопасности:

– неотказуемость или аппелируемость (от англ. *non-repudiation*) – способность удостоверять имевшее место действие или событие так, что эти события или действия не могли быть позже отвергнуты;

– подотчетность (от англ. *accountability*) – свойство, обеспечивающее однозначное прослеживание действий любого логического объекта;

– достоверность (от англ. *reliability*) – свойство соответствия предусмотренному поведению или результату;

– аутентичность или подлинность (от англ. *authenticity*) – свойство, гарантирующее, что субъект или ресурс идентичны заявленным [6].

В настоящее время, в органах власти, крупных компаниях и организациях (далее – организации) большое внимание уделяется вопросам создания систем обеспечения информационной безопасности (СОИБ). Эффективность функционирования таких сложных систем как СОИБ, зависит от сбалансированности и качества принимаемых решений (управляющих воздействий). Система обеспечения информационной безопасности должна своевременно и адекватно реагировать на возможные неблагоприятные ситуации. Для этого должен быть разработать механизм (система управления) своевременного обнаружения и оперативного устранения угроз информационной безопасности. Система управления информационной безопасности (СУИБ) должна выявлять уязвимости на самых

ранних стадиях, когда еще возможно их устранение с минимальными затратами ресурсов и усилий. Особое внимание в СУИБ должно быть уделено методам выявления и способам защиты жизненно важных, стратегических интересов компании [4; 5]

Информационная безопасность организации – это состояние защищённости информации, при которой обеспечивается ее конфиденциальность, целостность и доступность. Защите подлежит как информация ограниченного доступа, так и общедоступная информация [1]. Объектами защиты являются: объекты информатизации, включающие автоматизированные (информационные) системы различного уровня и назначения, средства и системы обработки информации и средства их обеспечения, а также помещения, предназначенные для ведения секретных (конфиденциальных) переговоров (выделенные (защищаемые) помещения).

Информационная безопасность организации достигается комплексом организационных и технических мер, направленных на защиту информации в соответствии с требованиями, предъявляемыми к защите соответствующего вида информации [8].

В статье предлагается методический подход к реализации процесса подготовки и обоснования решений на основе анализа стандартных ситуаций, возникающих в деятельности руководителей организаций, службы информационной безопасности и структурных подразделений по защите информации.

Постановку задачи сформулируем с учётом положений, изложенных в работе [2]. Пусть в процессе управления информационной безопасностью фиксируются отклонения отдельных показателей процесса обеспечения информационной безопасности (ОИБ) $M^n = \{m_i\}^n_{i=1}$ от требуемых значений. Причины отклонения W_x известны, а средства достижения требуемых значений заранее не определены. Такое состояние в управлении ОИБ в дальнейшем понимается как стандартная ситуация в ОИБ W.

Требуется по значениям m_i оценить сложившуюся ситуацию W (например, $W_{кр}$ – критическая, $W_{нд}$ – неудовлетворительная, $W_н$ – нормальная); найти первопричины g_x, обусловившие возникновение W; предложить альтернативные решения $\{r_i\}$; выбрать и обосновать оптимальное (рациональное) решение (R_j).

Цель решения задачи – вернуть систему ОИБ в состояние нормального функционирования (отвечающего, предъявляемым требованиям):

$$V(M^n) : W_{кр} \Longrightarrow W_н \, U \, W_{нд} \Longrightarrow W_{кр} \Longrightarrow W_н \, U \, W_{нд} \Longrightarrow W_н. \quad (1)$$

Формула управления упрощенно может быть представлена следующим выражением:

$$V(M^n) \subset Y(M^n), L(W), Q(m_i), G(R_j), \quad (2)$$

где $Y(M^n)$ – измерение вектора M^n; $L(W)$ – оценка ситуации; $Q(m_i)$ – поиск показателей первопричин, давших отклонение от требуемых значений; $G(R_j)$ – поиск класса решений R_j. Эта операция последовательно повторяется для уточнения класса R_j и выхода на операцию $R_{опт}$.

Результаты решения задачи могут быть представлены в виде диаграммы, изображенной на рисунке 1.

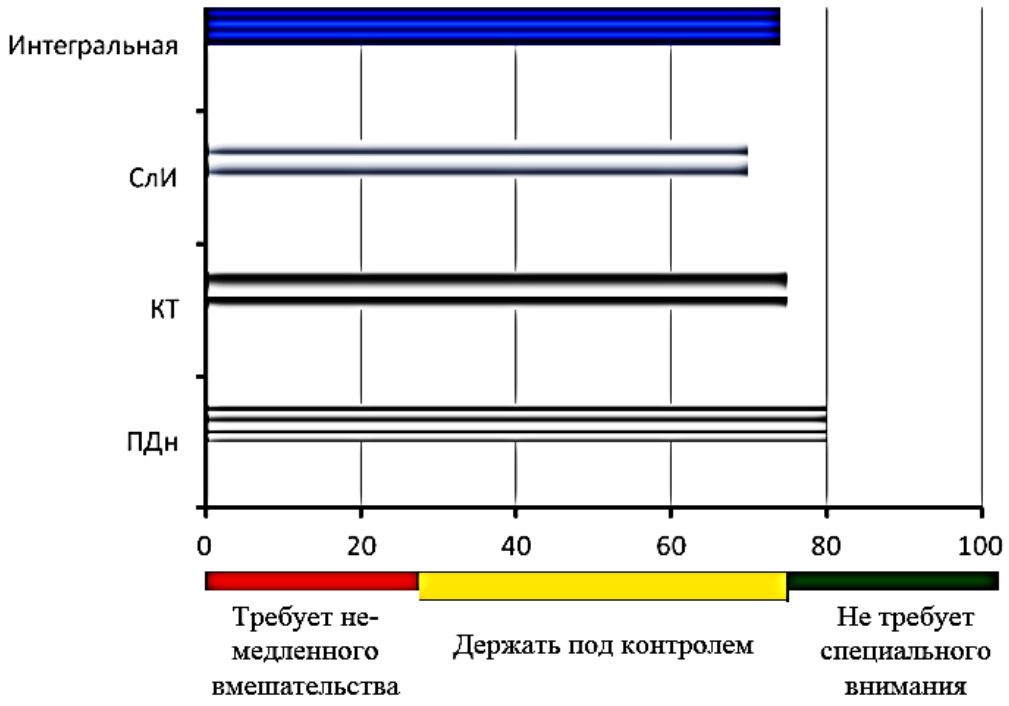

Рис. 1

На рисунке 1 приведены значения состояния защиты ПДн – персональных данных, КТ – коммерческой тайны, СлИ – служебной информации и интегральная оценка состояния информационной безопасности организации [7].

Таким образом, задача комплексной оценки состояния защиты информации в организации в общем случае заключается в определении соответствия фактического состояния системы обеспечения информационной безопасности предъявляемым требованиям и выработки решения на приведение системы в соответствие требованиям нормативных правовых актов и нормативных документов в области защиты информации.

Список литературы

1. Федеральный закон от 27.06.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Швед В.Г. Многоуровневая технология обеспечения качества АСУТ: Докторская диссертация. – СПб.: ВАТТ, 1999.

3. Макаров А.Д. Проблемы и концептуальные основы инвестиционной деятельности в оборонно-промышленном комплексе // М-во образования и науки Рос. Федерации, Гос. образоват. учреждение высш. проф. образования «С.-Петерб. гос. ун-т экономики и финансов». – СПб., 2004. – С. 27–64.

4. Макарова И.А. Механизм оптимизации инновационной политики на предприятии // Современные проблемы науки и образования. – №3. – 2012. – С. 262.

5. Макарова И.А. Совершенствование механизма управления инновациями на предприятиях высокотехнологичных секторов экономики // Вестник ИНЖЭКОНА. Серия «Экономика». – №5. – 2010. – С. 371–373.