

ЛАТЕНТНЫЕ ЭЛЕМЕНТЫ СИСТЕМЫ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ: ОПРЕДЕЛЕНИЕ И КЛАССИФИКАЦИЯ

В современных системах комплексной безопасности хозяйствующих субъектов помимо элементов (механизмов) защиты, имеющих открытый (публичный, явный) характер и непосредственно используемых персоналом (пользователями, субъектами защиты) и подразделением безопасности в процессе служебной деятельности, как правило, имеются и применяются на практике различные скрытые элементы защиты, носящие в основном фискальный характер.

Являясь объективной реальностью, такие недеклалируемые возможности, реализуемые специальными самостоятельными функциональными элементами (подсистемами), входящими в состав системы комплексной безопасности хозяйствующего субъекта, или интегрированные в какие-либо известные рядовому пользователю (традиционные) функциональные элементы (подсистемы) в виде специальных модулей, блоков или процедур, представляют определенный интерес для профессионального сообщества как предмет для публичного обсуждения, анализа и изучения.

подавляющее большинство элементов (механизмов) защиты носят открытый (публичный, явный) характер по отношению к потенциальному пользователю (субъекту защиты), что само по себе не является недостатком, а в ряде случаев просто необходимо для наиболее эффективного их использования, поскольку понимание и добросовестное выполнение пользователем (субъектом защиты) требований и процедур безопасности является залогом успешной деятельности по обеспечению безопасности.

Вместе с тем известность защитных механизмов пользователю (субъекту защиты) подразумевает, согласно общепринятой модели потенциального нарушителя, также их известность внутреннему (внешнему) нарушителю (злоумышленнику).

Это не является проблемной ситуацией, поскольку воспринимается как объективная реальность, которую принимают и с учетом которой действуют все субъекты безопасности, включая разработчиков механизмов и систем безопасности.

При этом всем известно, что помимо элементов (механизмов) защиты, имеющих открытый (публичный, явный) характер, существуют и применяются на практике различные латентные (скрытые, замаскированные) элементы защиты, выполняющие специфические функции безопасности, причем на абсолютно очевидных для профессионалов основаниях.

В русском языке слово «латентный» (от лат. *latens* (*latentis*) — скрытый, невидимый) используется, когда речь идет о каких-либо реально существующих или возможных скрытых, внешне не проявляющихся явлениях, факторах, признаках и т. п. [5]. Применительно к понятийному аппарату в области обеспечения объектовой безопасности слово «латентность» используется в отношении скрытых, не поддающихся непосредственному измерению или объективному прогнозированию свойств и особенностей защищаемого объекта или факторов угроз нанесения ему ущерба (вреда), определяющих условия его комплексной защиты и потенциально опасные последствия от возникновения угрожающей (чрезвычайной) ситуации на объекте или реализации угрозы [1, 3].

В области психологии, социологии, теории управления экономическими системами и администрирования слово «латентность» используется при рассмотрении особенностей скрытого деструктивного (маргинального) или конструктивного управления различными организациями или целевыми группами [2, 4].

В отношении скрытых (недекларируемых) свойств и возможностей систем безопасности какая-либо единая терминология и классификация до настоящего времени не введены и нормативно не закреплены.



В связи с этим предлагается ввести следующее определение латентного элемента системы комплексной безопасности хозяйствующего субъекта.

Элемент системы комплексной безопасности хозяйствующего субъекта (или входящей в ее состав подсистемы), наличие и функционирование которого сознательно скрываются разработчиком системы безопасности (службой безопасности) от пользователя (субъекта защиты) и неизвестны ему, не поддающийся обнаружению и/или нейтрализации с помощью официально имеющихся в распоряжении пользователя (субъекта защиты) технических (аппаратно-программных) средств и не имеющий с ним обратной связи, называется латентным.

Аналогичным образом можно определить и латентную подсистему системы комплексной безопасности хозяйствующего субъекта, являющуюся по сравнению с элементом более сложной и организованной сущностью. В связи с этим в настоящей статье, при отсутствии принципиальных различий или специальных примечаний, все суждения, сформулированные в отношении латентного элемента, являются приемлемыми также в отношении латентной подсистемы, входящей в состав системы комплексной безопасности хозяйствующего субъекта.

Предлагается ввести классификацию (не претендующую на полноту и исключительность) латентных элементов системы комплексной безопасности хозяйствующего субъекта исходя из следующих свойств и признаков:

- по степени интеграции в систему комплексной безопасности или ее подсистемы;
- по функциональному назначению (выполняемой функции);
- по степени управляемости;
- по возможности удаления (отключения);
- по наличию обратной связи с администратором системы;
- по возможности представления администратору системы результатов своей работы или отчетности;
- по статусу (охватываемой аудитории);
- по наличию моральной составляющей;
- по энергозависимости (ресурсозатратности);
- по количеству выполняемых функций;
- по характеру влияния на функции безопасности;
- по уровню (порядку) латентности.

Рассмотрим более подробно виды (типы) латентных элементов безопасности, исходя из предложенных признаков классификации.

1. По степени интеграции в систему комплексной безопасности хозяйствующего субъекта или ее подсистемы латентные элементы безопасности могут быть:

- резидентными, т. е. встроенными в подсистему или какой-либо блок (модуль, устройство) безопасности, входящие в состав системы комплексной безопасности хозяйствующего субъекта, и являющимися их неотъемлемой частью;
- нерезидентными, т. е. обособленными, представляющими собой самостоятельный продукт, который может при необходимости добавляться (инсталлироваться) в подсистему безопасности, входящую в состав системы комплексной безопасности хозяйствующего субъекта, или функционировать самостоятельно.

2. По функциональному назначению (выполняемой функции) латентные элементы безопасности классифицируются в соответствии с конкретной специализацией и непосредственным своим назначением.

Например, латентные элементы могут выполнять следующие функции:

- регистрации, мониторинга, контроля, наблюдения и т. п. за значимыми (критичными) для деятельности хозяйствующего субъекта процессами, объектами или событиями;



- обнаружения, активного или пассивного противодействия атакам или иным деструктивным воздействиям на защищаемые (контролируемые) процессы или ресурсы;
- создания и поддержания безопасной среды функционирования значимых (критичных) процессов или объектов;
- перехвата (получения) значимой информации;
- противодействия конкурентной разведке, создания и поддержания каналов дезинформации, а также другие функции.

3. По степени управляемости, т. е. предусмотренной конструктивно или разработчиком возможности администрирования, внесения/изменения каких-либо настроек или иного влияния на их работу в течение жизненного цикла, латентные элементы безопасности могут быть управляемыми и неуправляемыми.

4. По возможности удаления (отключения) латентные элементы безопасности соответственно могут быть удаляемыми (отключаемыми) и неудаляемыми (неотключаемыми).

5. По наличию обратной связи с администратором системы (специальным персоналом службы безопасности или иным уполномоченным лицом) латентные элементы безопасности могут быть с обратной связью и без обратной связи.

6. По возможности представления администратору системы (специальному персоналу службы безопасности или иному уполномоченному лицу) результатов своей работы или какой-либо отчетности, например, в виде визуальных сообщений об отмеченных событиях, сформированных файлах или протоколах (иных документах), выводимых на печать, латентные элементы безопасности могут быть фискальными и нефискальными.

7. По статусу (контролируемой, охватываемой аудиторией) латентные элементы безопасности могут быть объектовыми, отраслевыми, межотраслевыми и глобальными.

8. По наличию моральной составляющей и правомерности использования латентные элементы безопасности могут быть этичными и неэтичными.

9. По энергозависимости (ресурсозатратности) латентные элементы безопасности могут быть автономными и энерго-(ресурсо-)зависимыми.

10. По количеству выполняемых функций латентные элементы безопасности могут быть узкоспециализированными и универсальными.

11. По характеру влияния на функции и работоспособность системы комплексной безопасности хозяйствующего субъекта латентные элементы могут быть конструктивными (полезными, дружественными) и деструктивными (вредоносными, враждебными), если вызывают в системе комплексной безопасности, в которую они внедрены, какие-либо негативные последствия от выполнения возложенных на них функций.

Например, интуитивно понятно, что если при построении системы комплексной безопасности хозяйствующего субъекта используется импортное программное или аппаратное обеспечение, имеющее в своем составе неизвестные интегратору латентные элементы (недекларируемые возможности), существует риск деструктивного воздействия таких элементов на систему комплексной безопасности хозяйствующего субъекта. Мотивация такого воздействия может быть различной, в зависимости от статуса и значимости хозяйствующего субъекта. Примеры деструктивного воздействия, наблюдавшиеся в ходе военных и экономических конфликтов последнего времени, мировой общественности достаточно хорошо известны.

12. По уровню (порядку) латентности скрытые элементы безопасности могут быть 1-го, 2-го и 3-го порядка, независимо от их функциональной направленности.

Латентные элементы 1-го порядка — элементы, наличие (присутствие, функционирование) и назначение которых скрыто от персонала (субъектов защиты) хозяйствующего субъекта.

Установка (внедрение) этих элементов санкционируется руководством службы безопасности хозяйствующего субъекта. Администрирование (управление) такими элементами, осуществление обратной связи, возможность их удаления (отключения), а также обработка и последующее использование (представление руководству) результатов их работы относятся к компетенции службы безопасности хозяйствующего субъекта.

Латентные элементы 2-го порядка – элементы, наличие (присутствие, функционирование) и назначение которых скрыто не только от персонала (субъектов защиты), но и от неуполномоченного персонала службы безопасности хозяйствующего субъекта. Установка (внедрение) этих элементов санкционируется высшим менеджментом (руководством) хозяйствующего субъекта. Установка (внедрение), администрирование (управление) такими элементами, осуществление обратной связи, возможность их удаления (отключения), а также обработка и последующее использование (представление руководству) результатов их работы осуществляются непосредственно руководителями и/или особо доверенными (привилегированными) специалистами службы безопасности или иными уполномоченными лицами хозяйствующего субъекта.

Латентные элементы (подсистемы) 3-го порядка – элементы, наличие (присутствие, функционирование) и назначение которых скрыто от персонала (субъектов защиты), всего руководства и специалистов службы безопасности, а также от высшего менеджмента хозяйствующего субъекта. Установка (внедрение) таких элементов осуществляется научно-техническим персоналом (разработчиками) на этапе проектирования систем (подсистем) безопасности. При этом текущее администрирование (управление) такими элементами может осуществляться органами государственной власти и специальными службами (в соответствии с их компетенцией) по удаленным каналам доступа (управления) или не осуществляться вообще, если целью создания и функционирования латентного элемента является нефискальная постоянно действующая функция безопасности. В этом случае также может не осуществляться непосредственное использование результатов (отчетов, протоколов) их работы. Соответственно отсутствует обратная связь с такими элементами и возможность влияния на их работу. Удалить (исключить, отключить) такие элементы, даже силами разработчика, как правило, невозможно. Принципиальная возможность создания таких элементов определяется текущими достижениями в области науки и техники. Необходимость (целесообразность) их внедрения определяется органами государственной власти и специальными службами (в соответствии с их компетенцией).

При наличии достаточного воображения можно ввести дополнительные уровни латентности, например, более высокого порядка.

Основные признаки классификации латентных элементов 1-го, 2-го и 3-го порядка системы комплексной безопасности хозяйствующего субъекта представлены в таблице.

| Признаки классификации латентных элементов | Латентный элемент 1-го порядка | Латентный элемент 2-го порядка | Латентный элемент 3-го порядка |
|---|---|---|---|
| Наличие и назначение латентных элементов | Скрыто от персонала хозяйствующего субъекта | Скрыто от персонала, а также от неуполномоченного персонала службы безопасности хозяйствующего субъекта | Скрыто от персонала, всего руководства и специалистов службы безопасности, а также от высшего менеджмента хозяйствующего субъекта |



| | | | |
|---|--|--|--|
| Установка (внедрение) латентных элементов | Санкционируется руководством службы безопасности хозяйствующего субъекта | Санкционируется высшим менеджментом (руководством) хозяйствующего субъекта | Санкционируется органами государственной власти и специальными службами (в соответствии с их компетенцией) |
| Администрирование (управление), осуществление обратной связи, возможность удаления (отключения), обработка и последующее использование (представление руководству) результатов работы латентных элементов | Осуществляются службой безопасности хозяйствующего субъекта | Осуществляются непосредственно руководителями и/или особо доверенными | Осуществляются органами государственной власти и специальными службами (в соответствии с их компетенцией) по удаленным каналам доступа (управления) или не осуществляются вообще. Удалить (исключить, отключить) такие элементы, даже силами разработчика, как правило, невозможно |

В зависимости от вида и своего функционального назначения латентные элементы, принадлежащие одной системе комплексной безопасности хозяйствующего субъекта, могут, если это целесообразно и предусмотрено разработчиком системы, взаимодействовать между собой на различных иерархических уровнях. Такое взаимодействие называется внутрисистемным и может осуществляться как «по горизонтали», так и «по вертикали».

Под взаимодействием «по горизонтали» понимается какая-либо связь (в том числе использование результатов работы друг друга) латентных элементов, принадлежащих одному иерархическому уровню в структуре системы комплексной безопасности хозяйствующего субъекта и имеющих одинаковый порядок латентности.

Под взаимодействием «по вертикали» понимается какая-либо связь (в том числе использование результатов работы друг друга) латентных элементов, принадлежащих разным иерархическим уровням в структуре системы комплексной безопасности хозяйствующего субъекта или имеющих различный порядок латентности.

Кроме внутрисистемного взаимодействия может осуществляться межсистемное взаимодействие латентных элементов, принадлежащих различным системам комплексной безопасности различных хозяйствующих субъектов. Межсистемное взаимодействие может осуществляться «по горизонтали» и «по вертикали» так, как это определено для внутрисистемного взаимодействия латентных элементов.

В зависимости от функционального назначения латентные элементы могут быть управляемыми и неуправляемыми.

Под управлением латентными элементами в общем случае подразумевается сознательное и целенаправленное воздействие на их работу (например, посредством изменения настроек или параметров функционирования) со стороны уполномоченных лиц и/или других латентных элементов системы комплексной безопасности хозяйствующего субъекта или элементов каких-либо систем управления более высокого иерархического уровня.

Исследуя принципы и практику построения современных систем комплексной безопасности хозяйствующих субъектов, а также следуя элементарной логике и принципам целесообразности, можно утверждать, что большинство латентных элементов 1-го и 2-го порядков, как правило,



являются управляемыми, что для достижения поставленных целей эффективного обеспечения безопасности представляется вполне разумным.

Напротив, латентные элементы 3-го порядка, в силу высочайшей степени скрытости и возможной значительной удаленности от уполномоченного лица, могут быть неуправляемыми. В свою очередь, такие латентные элементы могут быть удаляемыми и неудаляемыми.

Не рассматривая конкретные виды и типы управляющих воздействий, можно отметить, что управление латентными элементами может быть непосредственным и опосредованным. Исходя из смыслового значения указанных слов нетрудно представить основные принципы такого управления.

Предложенная в настоящей статье система взглядов (концепция) и некоторый понятийный аппарат, описание и классификация латентных (скрытых от неуполномоченных лиц) элементов (подсистем) системы комплексной безопасности хозяйствующего субъекта не претендуют на полноту и исключительность. При их разработке автор руководствовался пониманием того, что в настоящее время различные латентные элементы являются объективной реальностью и вызывают определенный интерес у разработчиков и потребителей средств безопасности. Поэтому на современном этапе зрелости общества и развития знаний о принципах построения, методах, технологиях и средствах обеспечения комплексной безопасности различных объектов латентные элементы могут являться предметом публичного и квалифицированного обсуждения, анализа и изучения.

СПИСОК ЛИТЕРАТУРЫ:

1. ГОСТ Р 53704-2009. Национальный стандарт Российской Федерации. Системы безопасности комплексные и интегрированные. Общие технические требования (утвержден и введен в действие Приказом Ростехрегулирования от 15.12.2009 № 1140-ст).
2. Минзов А. С. Маргинальное управление: сущность, цели, методы управления и манипулирования. URL: <http://www.dist.i-b-b.su>.
3. РД 25.03.001-2002. Системы охраны и безопасности объектов. Термины и определения.
4. Савченко А. В. Латентное управление: сущность и механизм использования. АКД, М., 2008. — 23 с.
5. Современный толковый словарь русского языка / Гл. ред. С. А. Кузнецов. СПб.: Норинт, 2001. — 960 с.