DOI: 10.18372/2410-7840.19.11683
УДК 004.056.53

ДЕСКРИПТИВНЫЙ АНАЛИЗ АНАЛОГИЙ МЕЖДУ СИСТЕМАМИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ И МАССОВОГО ОБСЛУЖИВАНИЯ

Владимир Мохор, Александр Бакалинский, Александр Богданов, Василий Цуркан

Устанавливается, что на сегодняшний день ни один из существующих международных стандартов не содержит конкретных методик формирования проектных требований к системе управления информационной безопасностью применительно к конкретной организации. Для преодоления этого ограничения рассматривается возможная аналогия систем массового обслуживания и систем управления информационной безопасностью. Проведение дескриптивного анализа возможных аналогий осуществляется путем сравнения состава и общей функциональной модели системы массового обслуживания. На основании такого сравнения устанавливается возможность использования математического аппарата теории систем массового обслуживания для формирования проектных требований к системе управления информационной безопасностью. Это позволит разработать модель такой системы. С ее помощью станет возможным определение степени важности того или иного аспекта информационной безопасности применительно к конкретной организации.
Ключевые слова: *риск информационной безопасности, система управления информационной безопасностью, система массового обслуживания, поток рисков, дескриптивный анализ.*

Постановка проблемы. Для обеспечения информационной безопасности, зрелые компании внедряют у себя системы управления информационной безопасностью (СУИБ), которые строятся, как правило, на основе требований, изложенных в международных стандартах серии ISO/IEC 27k. В частности, в стандарте ISO/IEC 27001:2013 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования» [1]. Сразу отметим, что ни один из существующих стандартов не содержит конкретных методик формирования проектных требований к СУИБ (то есть, применительно к конкретной организации). Вместе с тем, часто речь идет о тех или иных аспектах информационной безопасности (ИБ), которые должны быть внедрены во всей организации или по отношению к конкретному бизнес-процессу. В таком случае, для того, чтобы понять, какие аспекты являются наиболее важными, какие характеристики должны быть реализованы при создании СУИБ желательно иметь некоторую формальную модель этой конкретной СУИБ. Исследование параметров такой модели может дать понимание того, на какие аспекты ИБ необходимо обращать пристальное внимание, а какие аспекты не являются принципиально важными. Для того, чтобы понять, какой именно вид может иметь формальная модель СУИБ, какие из формальных методов применимы при моделировании СУИБ, необходимо установить какому из видов формальных систем она аналогична. Если аналогии удастся выявить, то тогда можно предположить, что формальные методики проектирования, известные для систем-аналогов, удастся адаптировать к задачам создания СУИБ.

Изложение основного материала исследования. С целью выявления наиболее общих аналогий между СУИБ и известными формальными системами рассмотрим более подробно основные качества СУИБ. Согласно [1] система управления информационной безопасностью – это «та часть общей системы управления организации, которая основывается на оценке рисков. Ею, как частью общей системы управления, создается, реализуется, эксплуатируется, осуществляется мониторинг, пересматривается, сопровождается и совершенствуется обеспечение информационной безопасности». Из этого определения следует, что все и любые СУИБ можно рассматривать как класс систем, предназначенных для многоразового решения однотипных, в определенном смысле, задач. Такая трактовка наводит на мысль об аналогии между СУИБ и системой массового обслуживания (СМО), в которой требования на выполняемые работы проявляются в виде событий информационной безопасности.

Отметим, что в общем случае последовательность требований на обслуживание, имеющих вид событий/рисков информационной безопасности, является случайной, как по времени проявления событий/рисков, так и по типу таких событий/рисков. Случайность последовательности событий/рисков, обслуживаемых СУИБ, является еще одним аспектом аналогии между СУИБ и СМО.

Согласно ISO/IEC 27001:2013 все события информационной безопасности могут быть разбиты на отдельные группы в зависимости от того, в рамках каких пунктов Приложения А стандарта [1] они реализуются. В частности, это могут быть, например, события в ИТ-инфраструктуре организации, факты несанкционированного пересечения периметра безопасности, кадровые проблемы, несоблюдение тех или иных норм законодательства, чрезвычайные происшествия и т.д. Обработкой событий информационной безопасности, относящихся к каждой из таких отдельных групп, занимаются, как правило, специально подготовленные команды специалистов, а иногда – внешние организации, вплоть до правоохранительных структур. Каждую из таких отдельных команд можно рассматривать, как отдельный канал обслуживания событий/рисков информационной безопасности, специализирующийся на событиях/рисках определенной группы, но, в принципе, способный обслуживать события/риски, относящиеся и другим группам. Таким образом, видим наличие каналов обработки требований, и в этом суть еще одной аналогии между СУИБ и СМО.

Очевидно, что события информационной безопасности влекут за собой последствия в виде ущерба определенного размера H, возникновение которого связано с некоторой вероятностью p. В то же время, известно, что комбинация размера ущерба и вероятности его возникновения есть риск R, определяемый в простейшем случае соотношением

$$R = H \cdot p.$$

В таком случае можно говорить, что СУИБ есть СМО, в которой требования на выполняемые работы проявляются в виде возникновения рисков информационной безопасности, а суть выполняемых работ – обслуживание этих рисков в соответствии с рекомендациями серии стандартов ISO/IEC 27k.

Обслуживание понимается в том смысле, что СУИБ оценивается уровень возникающих рисков и обрабатываются те из них, для которых оценка риска оказывается превышающей заданный порог. Все остальные события документируются, но СУИБ не переходит в состояние их обработки. Иными словами, СУИБ просто игнорируются такие события. Если в качестве отдельного, скажем так – нулевого события информационной безопасности, рассматривать еще и факт отсутствия каких-либо событий информационной безопасности, то очевидно, что такое нулевое событие не требует никакой обработки, то есть оно игнорируется. Таким образом, можем констатировать, что механизм обслуживания рисков в СУИБ должен обслуживать все входящие риски, но предполагает два непересекающихся класса состояний обслуживания: обработка и игнорирование. В принципиальной способности СУИБ обслужить любой риск проявляется еще одна аналогия между СУИБ и СМО.

Приведенный ряд аналогий между СУИБ и СМО является достаточным для констатации возможности интерпретации СУИБ в качестве СМО. В связи с замеченными аналогиями, как проекции СУИБ на СМО, попытаемся выявить аналогии в отображении СМО на СУИБ.

По определению [3], системы массового обслуживания – это такие системы, в которые в случайные моменты времени поступают требования на выполняемые работы, обслуживание. При этом поступившие заявки обслуживаются с помощью имеющихся в распоряжении системы каналов обслуживания. Рассмотрим состав СМО, ее обобщенную функциональную модель (см., например, [4], рис. 1), а также возможность её интерпретации в контексте СУИБ. В состав СМО входят генератор заявок, диспетчер, узел обслуживания с каналами обслуживания, терминатор (узел отказов, уничтожитель заявок) и очередь.

1. Генератор заявок в СМО – это объект, порождающий заявки [5-8]. Для СУИБ генератором заявок выступают экзогенные факторы (клиенты, контракторы, поставщики, законодатель страны пребывания, злоумышленники, правоохранительные органы, регуляторы) или/и эндогенные факторы (персонал, требования внутренних приказов, стандартов, корпоративные требования, взаимосвязи между подразделениями организации, выход из строя или не корректная работа оборудования и т. д.), порождающие риски, каждый из которых нуждается в обслуживании (обработать либо игнорировать).

2. Очередь в СМО – это некий механизм накопления заявок, которые выстраиваются в последовательности [5-8]. Правило формирования последовательности заявок определяется дисциплиной очереди.

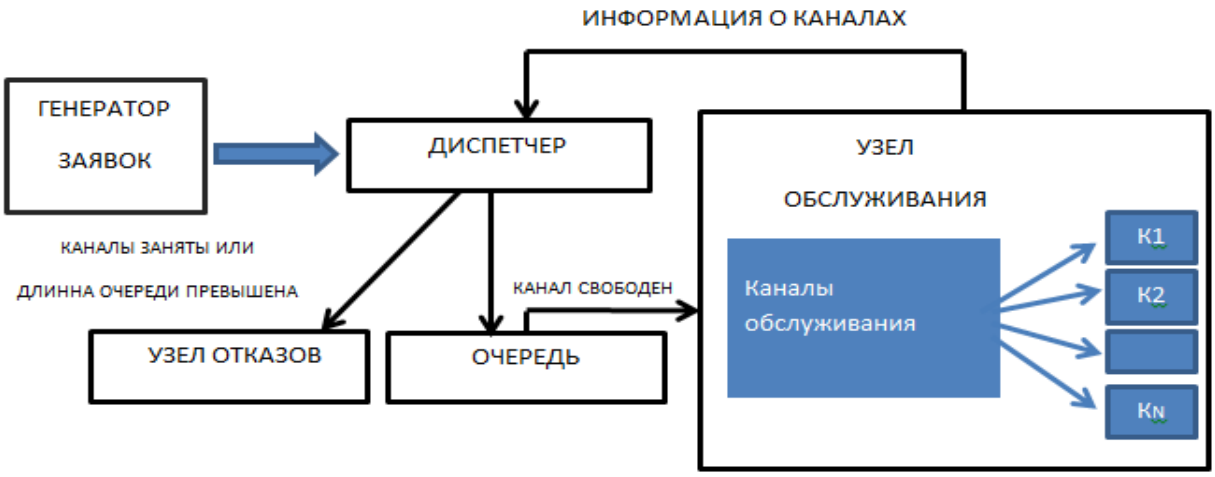

Рис. 1. Состав и обобщенная функциональная модель СМО

В случае СУИБ также предусматривается наличие механизма формирования очереди, который накапливает события/риски ИБ в очереди на обслуживание. Правилом формирования очереди выступает приоритетность заявок (в роли приоритета выступает уровень риска).

3. Отказ от обслуживания. Известно [7-8], что СМО делятся на два класса: СМО «с отказами» и СМО «с очередью». В СМО с «отказами» заявка, поступившая в момент, когда все каналы обслуживания заняты, получает отказ, покидает систему и в дальнейшем процессе обслуживания не участвует. В случае же «СМО с очередью» заявка, заставшая все каналы занятыми, не покидает систему, а направляется в очередь и ожидает, пока не освободится соответствующий канал. Отказ от обслуживания в случае «СМО с очередью» может произойти, например, при ограничении длинны очереди или времени пребывания в очереди.

В СУИБ не может быть ограничено время ожидания обслуживания, потому что необходимо рассмотреть все риски ИБ, о которых стало известно системе [1]. Для СУИБ недопустимо отказывать в обслуживании в связи с занятостями каналов обслуживания (занятостью сотрудников подразделения ИБ). Таким образом, можно сделать вывод о том, что СУИБ относится к классу СМО с неограниченной очередью, то есть нет ограничений ни по времени обслуживания, ни по длине очереди.

4. Диспетчер в СМО – это механизм принятия решений, необходимых в связи с обслуживанием заявки [6]. Диспетчер в СМО:

– принимает заявки;

– принимает информацию от узла обслуживания о свободных/занятых каналах;

– направляет заявки в каналы обслуживания, если есть свободные каналы;

– формирует очередь, если каналы заняты;

– следит за временем работы системы;

– формирует отказы на обслуживание.

Рассмотрим задачи и порядок работы диспетчера в СУИБ. В общем случае в СУИБ должен быть реализован некий механизм, задачей которого есть приём заявок на обслуживание. В зависимости от оценки уровня риска ИБ, диспетчер формирует очередь заявок. После этого, он распределяет заявки между каналами (исполнителями, в роли которых выступают сотрудники подразделения ИБ) и контролирует временные характеристики обслуживания заявки, ведет отчет о поступивших заявках, имеет актуальную информацию о занятости сотрудников, которые обслуживают заявки.

Более того, в международном стандарте ISO/IEC 27035-1:2016 «Информационные технологии. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 1. Принципы управления инцидентами» определена необходимость существования Команды реагирования на инциденты информационной безопасности, которая определяется, как команда надлежащим образом квалифицированных и надежных членов организации, которая обрабатывает инциденты информационной безопасности в процессе их жизненного цикла [10]. И, именно диспетчер СУИБ (сотрудник HelpDesk/ИБ) в случае классификации события, как инцидента (реализующийся или реализованный риск ИБ), инициирует начало активной работы этой команды.

Одним из примеров реализации диспетчера в СУИБ, является HelpDesk (Service Desk). HelpDesk (Service Desk) предназначены для автоматизации обработки запросов клиентов. Большинству клиентов удобнее получать поддержку

по e-mail или на web-сайте поставщика, поэтому большинство HelpDesk системы на сегодняшний день являются онлайновыми, либо предоставляют клиентский web-интерфейс.

Основным компонентом любого HelpDesk-решения (см., например [5], рис. 2) является система управления запросами (или инцидентами, тикетами, багами).

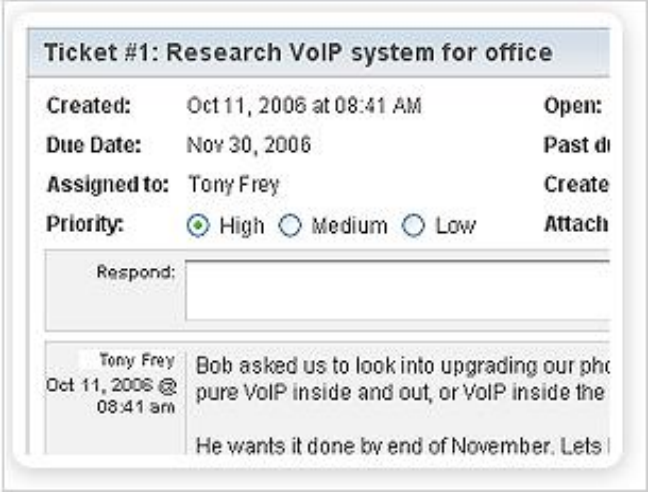

Рис. 2. Пример использования системы управления запросами HelpDesk-решения

При поступлении запроса от клиента (по телефону, по e-mail, через web-сайт), в системе автоматически создается «тикет», который, в зависимости от его содержания и важности, ставится в очередь одному из сотрудников службы поддержки и/или ИБ. Сотрудник службы поддержки и/или ИБ и тот уже работает с клиентом над решением проблемы. В ходе этого процесса статус тикета обновляется, и руководитель службы поддержки и/или ИБ может контролировать как сотрудники службы поддержки справляются с нагрузкой.

Кроме системы тикетов HelpDesk-система может включать следующие дополнительные компоненты:

– база клиентов;

– база знаний для поиска готовых решений;

– web-портал для клиентов (где они могут создавать запросы и контролировать их статус);

– база договоров на обслуживание (SLA = Service Level Agreement);

– база продуктов.

Кроме поддержки клиентов, системы Service Desk получили широкое применение в ИТ-отделах крупных компаний, которые используют Service Desk для управления ИТ инфраструктурой (ITSM). Поэтому, многие Service Desk системы содержат специализированные функции для управления ИТ, и как следствие решение вопросов, связанных с ИБ:

– учет конфигураций (каталог ИТ ресурсов компании, их версии и настройки);

– учет проблем (проблемы – это повторяющиеся инциденты);

– учет изменений (например, обновлений версий ПО) [5].

Итак, общее понимания задач, возлагаемых на диспетчера СУИБ, и анализ примеров реализации диспетчера СУИБ в конкретных системах, дает все основания утверждать наличие полной аналогии между диспетчером СМО и диспетчером СУИБ как по выполняемым задачам, так и по последовательности работы.

5. Узел обслуживания. В СМО узел обслуживания решает задачу преобразования входной заявки клиента в результат пожеланий клиента. Узел обслуживания может состоять из одного обслуживающего устройства (одноканальная СМО) либо из нескольких (многоканальная СМО). Если число обслуживающих устройств больше единицы, то должен быть указан порядок их расположения. Так, если обслуживающие устройства выполняют параллельно обработку сразу нескольких требований, то речь идет о многоканальной СМО. Если процесс обслуживания требований состоит из нескольких этапов, выполняемых последовательно друг за другом на различных обслуживающих устройствах, то такую систему называют многофазной. Каждый канал имеет три состояния: свободен, занят, не работает [6, 8].

В СУИБ, узел обслуживания существует с целью решения задачи по определению, является ли событие ИБ риском, если – да, то – оцениванию уровня рисков ИБ и принятия дальнейшего решения по целесообразности обработки рисков с целью приведения их к допустимому значению. Как видим, процесс обработки риска в СУИБ состоит из нескольких этапов, выполняемых последовательно друг за другом, что аналогично работе многофазной СМО.

Рассмотрев состав СМО, ее обобщенную функциональную модель и установив ряд структурных и функциональных аналогий, остановимся на возможности интерпретаций основных характеристик СМО в контексте СУИБ.

Как отмечено, например, в работах [6-9], основными характеристиками системы массового обслуживания любого вида являются:

1. Входящий поток требований (заявок) на обслуживание.
2. Дисциплина очереди.
3. Механизм обслуживания.

Для каждой из этих характеристик рассмотрим аналогии между СМО и СУИБ.

1. Входящий поток требований (заявок) на обслуживание.

Как сказано, например, в [8], при исследовании систем массового обслуживания входящий поток заявок на обслуживание обычно считают пуассоновским с интенсивностью λ. Это означает, что требования поступают в случайные моменты времени, причем вероятность появления одного требования в интервале от $t+\Delta t$ равна $\lambda\Delta t$ и не зависит от t, а вероятность появления в этом интервале двух и более требований пренебрежимо мала. Такие предположения являются достаточно обоснованными для многих практических случаев, в частности для событий информационной безопасности такие предположения являются предельным случаем понятия динамического множества актуальных угроз [11] при $\Delta t \to 0$.

При этом, как опять таки отмечено в [6, 8], длительности обслуживания отдельных заявок могут предполагаться случайными с экспоненциальным законом распределения и средним временем обслуживания $1/\mu$, где μ-интенсивность обслуживания. Это означает, что вероятность окончания обслуживания очередной заявки в интервале от t до $t+\Delta t$ не зависит от t и равна $\mu\cdot\Delta t$.

Таким образом, для того, чтобы контекст создания СУИБ мог быть содержательно интерпретирован в виде задачи массового обслуживания необходимо определить вероятностные характеристики входного потока рисков. При этом входным потоком рисков будем называть случайную последовательность рисков, возникающих на входе СУИБ вследствие проявления соответствующих случайных событий информационной безопасности.

2. Дисциплина очереди.

Дисциплиной очереди в теории систем массового обслуживания называют совокупность правил, регулирующих формирование, движение и распад очереди [6, 8]. Дисциплина очереди в СМО определяет принцип, в соответствии с которым поступающие на вход обслуживающей системы требования подключаются из очереди к процедуре обслуживания.

Все принципы организации дисциплины очереди можно разбить на группы:

1. Первая группа – выбор заявок из очереди осуществляется в порядке поступления.

2. Вторая группа – выбор заявок осуществляется на основании дополнительной информации о времени выполнения задания или обработки заявки. Каждая заявка, поступившая в систему, должна нести в себе информацию о необходимом времени для ее обслуживания.

3. Третья группа – выбор заявок осуществляется на основании вычисляемого оставшегося времени пребывания в системе.

4. Четвертая группа – выбор заявок из очереди осуществляется в случайном порядке.

5. Пятая группа реализует обслуживания заявок с прерыванием, то есть заявка, обслуживаемая в данный момент и находящаяся в канале обслуживания, может быть снята с обслуживания, а канал будет предоставлен другой заявке.

В зависимости от конкретных особенностей СУИБ возможна любая из этих дисциплин очереди. Но, кроме того, возможны и другие дисциплины, в частности, в некоторых видах СМО отбор заявок на обслуживание осуществляется по определенным критериям приоритета [6-9]. В СУИБ аналогом приоритета выступает уровень риска ИБ (чем выше уровень риска, тем выше приоритет), а аналогией сортировки по приоритету, является процесс ранжирования рисков ИБ в зависимости от их уровня, необходимость чего определена в п.6.1.2 e2) международного стандарта ISO/IEC 27001:2013. В критических случаях, когда реализуемая угроза может нанести большой ущерб может реализовываться вариант с прерыванием, то есть большая часть сил подразделения ИБ начинает заниматься вновь возникшим риском, откладывая рассматриваемый риск на потом.

Таким образом, для СУИБ дисциплина очереди является так же, как и для СМО, обязательной характеристикой. Для организации дисциплины очереди в СУИБ используется группа принципов организации обслуживания заявок, в которой допускается прерывание процесса обслуживания заявки (риска) в случае поступления заявки на обслуживание риска с более высоким уровнем (приоритета).

3. Механизм обслуживания.

Механизм обслуживания определяется, в основном, характеристиками процедуры обслуживания.

К характеристикам процедуры обслуживания относятся:

– количество каналов обслуживания (N);

– продолжительность процедуры обслуживания (вероятностное распределение времени обслуживания требований);

– количество требований, удовлетворяемых в результате выполнения каждой такой процедуры (для групповых заявок);

– вероятность выхода из строя обслуживающего канала [6].

Результаты сравнения характеристик процедуры обслуживания СМО и СУИБ с целью выявления аналогий между ними приведены в табл. 1.

Таблица 1

Сравнение характеристик процедуры обслуживания СМО и СУИБ

Характеристики процедуры обслуживания СМО	**Характеристики процедуры обслуживания СУИБ**	**Вывод**
Количество каналов обслуживания (*N*)	Количество специалистов, привлеченных к обработке рисков ИБ	Совпадает
Продолжительность процедуры обслуживания (вероятностное распределение времени обслуживания требований)	Продолжительность обработки единичного риска ИБ	Совпадает
Количество требований, удовлетворяемых в результате выполнения каждой такой процедуры (для групповых заявок)	Заявки приходят дискретно, т.е. информация о рисках поступает поочерёдно, но каждый риск может быть направлен на нарушение одного или нескольких свойств ИБ. Таким образом, количество требований равно количеству свойств ИБ, подвергаемых риску, который поступил на обслуживание	Совпадает
Вероятность выхода из строя обслуживающего канала	Вероятность выхода из строя обслуживающего канала (болезнь сотрудника, отказ оборудования)	Совпадает

Из рассмотрения табл. видно полное совпадение механизма обслуживания СМО и СУИБ, что нашло своё отражение в совпадении характеристик процедуры обслуживания этих двух типов систем, а также полное совпадение демонстрирует и структура обслуживающей системы, которая использует разные методы работы.

Следует отметить дополнительно, что время обслуживания заявки (обработки риска) зависит от характера самой заявки или требований клиента (величины риска, времени, необходимого для проведения мероприятий по его обработке) и от состояния и возможностей обслуживающей системы (подразделения ИБ). В ряде случаев нужно также учитывать вероятность выхода из строя обслуживающего канала по истечении некоторого ограниченного интервала времени. Эта характеристика СМО может быть моделирована как поток отказов, имеющий приоритет перед всеми другими заявками. Те же рассуждения полностью применимы и для СУИБ.

Выводы. На основе рассмотрения структуры СМО и анализа её функциональной модели установлено структурная и функциональная аналогия между СМО и СУИБ. В частности, основные элементы этих систем сопоставимы и решают подобные задачи, и в первом приближении СУИБ можно рассматривать как многофазную СМО с ожиданием и неограниченной очередью. Из этой аналогии следует возможность постановки и решения задач, ассоциированных с СУИБ, как задач массового обслуживания, а СМО можно рассматривать как формальную модель СУИБ. Очевидно, что исследование параметров такой модели может открыть путь и к пониманию тех аспектов ИБ, на которые необходимо обращать пристальное внимание в жизненном цикле управления информационной безопасностью.

ЛИТЕРАТУРА

[1]. Information technology. Security techniques. Information security management systems. Requirements : ISO/IEC 27001:2013. Second edition 2013-10-01. Geneva, P. 23, 2013.

[2]. "Понятие системы управления информационной безопасностью". [Электронный ресурс]. Режим доступа: http://globaltrust.ru/ru/uslugi/vnedrenie-sistem-upravleniya-informacionnoi-bezopasnostyu/ponyatie-sistemy-upravleniya-informacionnoi-bezopasnostyu. [Дата доступа: январь 2017].

[3]. "Элементы теории массового обслуживания". [Электронный ресурс]. Режим доступа: math.immf.ru/lections/206.html. [Дата доступа: январь 2017].

[4]. "Системы массового обслуживания". [Электронный ресурс]. Режим доступа: http://eos.ibi.spb.ru/umk/11_4/5/5_R0_T6.html. [Дата доступа: январь 2017].

[5]. "Что такое Helpdesk (Service Desk)?". [Электронный ресурс]. Режим доступа: http://www.helpdeski.ru/tags/helpdesk. [Дата доступа: январь 2017].

[6]. Е. Вентцель, *Исследование операций: задачи, принципы, методология*. М.: Издательство «Наука»: Главная редакция физико-математической литературы, 1988, 132 с.

[7]. Е. Вентцель, *Теория вероятностей*. М.: Издательство «Наука»: Главная редакция физико-математической литературы, 1969, 515 с.

[8]. Б. Гнеденко, *Введение в теорию массового обслуживания*. М.: Букинист, 2012, 400 с.

[9]. Ю. Коршунов, *Математические основы кибернетики*. М.: Энергия, 1980, 424 с.

[10]. Information technology. Security techniques. Information security incident management. Part 1: Principles of incident management: ISO/IEC 27035-1:2016. – First edition 2016-11-01. Geneva, P. 21, 2016.

[11]. В. Мохор, А. Богданов, О. Крук, В. Цуркан, "Построение оценок рисков безопасности информации на основе динамического множества актуальных угроз", *Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова,* №56, С. 87-99, 2010.

REFERENCE

[1]. Information technology. Security techniques. Information security management systems. Requirements : ISO/IEC 27001:2013. Second edition 2013-10-01. Geneva, P. 23, 2013.

[2]. "The concept of information security management system". [Online]. Available: http: //globaltrust. ru/ ru/uslugi/vnedrenie-sistem-upravleniya-informacionnoi- bezopasnostyu/ ponyatie- sistemy- upravleniya-informacionnoi-bezopasnostyu. [Accessed: Jan-2017].

[3]. "Elements of queuing theory". [Online]. Available: math.immf.ru/lections/206.html. [Accessed: Jan-2017].

[4]. "Queuing Systems". [Online]. Available: http://eos. ibi. spb. ru/ umk/ 11_4/ 5/ 5_R0_T6. html. [Accessed: Jan-2017].

[5]. "What is Helpdesk (Service Desk)?". [Online]. Available: http:// www. helpdeski. ru/ tags/ helpdesk. [Accessed: Jan-2017].

[6]. E. Venttsel, *Operations research: objectives, principles, methodology*. Moscow: Nauka, 1988, 132 p.

[7]. E. Venttsel, *Probability theory*. Moscow: Nauka, 1969, 515 p.

[8]. B. Gnedenko, I. Kovalenko, *Introduction to queuing theory*. Moscow: Bukinist, 2012, 400 p.

[9]. Iu. Korshunov, *Mathematical Foundations of Cybernetics*. Moscow: Energiia, 1980, 424 p.

[10]. Information technology. Security techniques. Information security incident management. Part 1: Principles of incident management: ISO/IEC 27035-1:2016. – First edition 2016-11-01. Geneva, P. 21, 2016..

[11]. V. Mokhor, A. Bohdanov, O. Kruk, V. Tsurkan, "Building a risk assessment of information security based on dynamic set of actual threats", *Collection of scientific works Institute of Modelling Problems in Power Engineering*, no. 56, P. 87-99, 2010.

ДЕСКРИПТИВНИЙ АНАЛІЗ АНАЛОГІЙ МІЖ СИСТЕМАМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА МАСОВОГО ОБСЛУГОВУВАННЯ

Встановлюється, що на сьогоднішній день жоден з існуючих міжнародних стандартів не містить конкретних методик формування проектних вимог до системи управління інформаційною безпекою стосовно конкретної організації. Для подолання цього обмеження розглядається можлива аналогія систем масового обслуговування та систем управління інформаційною безпекою. Проведення дескриптивного аналізування можливих аналогій здійснюється шляхом порівняння будови та загальної функціональної моделі системи масового обслуговування. На основі такого порівняння встановлюється можливість використання математичного апарату теорії систем масового обслуговування для формування проектних вимог до системи управління інформаційною безпекою. Це дозволить розробити модель такої системи. За її допомогою стане можливим визначення ступеня важливості того чи іншого аспекту інформаційної безпеки стосовно конкретної організації.

Ключові слова: ризик інформаційної безпеки, система управління інформаційною безпекою, система масового обслуговування, потік ризиків, дескриптивний аналіз.

DESCRIPTIVE ANALYSIS OF ANALOGIES BETWEEN INFORMATION SECURITY MANAGEMENT AND QUEUING SYSTEMS

It is established that none of the existing international standards contains specific methods for the development of project requirements for the information security management system applied to a particular organization for now. To overcome this limitation it is considered a possible analogy of queuing systems and information security management systems. A descriptive analysis of possible analogies is carried out by comparing the composition and the general functional model of the queuing system. On the basis of this comparison, it is established that the mathematical apparatus of the theory of queuing systems can be used to formulate project requirements for the information security management system. This will allow the development of the model of such system. It will be possible to determine sensitivity of different aspects of information security applied to a particular organization with its help.

Keywords: information security risk, information security management system, queuing systems, flow of risks, descriptive analysis.

Мохор Владимир Владимирович, доктор технических наук, профессор, директор Института проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины.
E-mail: v.mokhor@gmail.com
Мохор Володимир Володимирович, доктор технічних наук, професор, директор Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України.
Mokhor Volodymyr, doctor of engineering science, professor, Director of Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine.

Бакалинский Александр Олегович, заместитель заведующего кафедрой Института специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского».
E-mail: baov@meta.ua
Бакалинский Олександр Олегович, заступник завідувача кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
Bakalynskyi Oleksandr, deputy head of department, Institute of special communications and information security National technical university of Ukraine «Igor Sikorsky Kyiv polytechnic institute».

Богданов Александр Михайлович, доктор технических наук, профессор, заведующий кафедрой Института специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского».
E-mail: a_m_bogdanov@inbox.ru
Богданов Олександр Михайлович, доктор технічних наук, професор, завідувач кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
Bohdanov Oleksandr, doctor of engineering science, professor, head of department, Institute of special communications and information security National technical university of Ukraine «Igor Sikorsky Kyiv polytechnic institute».

Цуркан Василий Васильевич, кандидат технических наук, доцент кафедры Института специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского».
E-mail: v.v.tsurkan@gmail.com
Цуркан Василь Васильович, кандидат технічних наук, доцент кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
Tsurkan Vasyl, candidate of engineering science, associate professor, Institute of special communications and information security National technical university of Ukraine « Igor Sikorsky Kyiv polytechnic institute».

DOI: 10.18372/2410-7840.19.11435
УДК 621.391:519.2

НИЖНІ МЕЖІ ІНФОРМАЦІЙНОЇ СКЛАДНОСТІ КОРЕЛЯЦІЙНИХ АТАК НА ПОТОКОВІ ШИФРИ НАД ПОЛЯМИ ПОРЯДКУ 2^r

Антон Олексійчук, Михайло Поремський

Кореляційні атаки відносяться до найбільш потужних атак на потокові шифри, а методи побудови таких атак та обґрунтування стійкості потокових шифрів відносно них утворюють розвинутий напрям сучасної криптології. Протягом останніх років у зв'язку з появою словоорієнтованих потокових шифрів спостерігається розвиток методів побудови кореляційних атак, що базуються на розв'язанні систем лінійних рівнянь зі спотвореними правими частинами над скінченними полями або кільцями лишків порядку $q \geq 2$. *В даній статті досліджується два таких методи, перший з яких полягає у розв'язанні зазначених систем рівнянь над полями порядку* 2^r, *де* $r \geq 2$, *а другий – у розв'язанні аналогічних систем рівнянь над полем з двох елементів. Отримано неасимптотичні нижні межі інформаційної складності зазначених атак, які уточнюють раніше відому евристичну оцінку. Отримані результати можуть бути використані при обґрунтуванні стійкості словоорієнтованих потокових шифрів відносно сучасних кореляційних атак.*
Ключові слова: *потоковий шифр, кореляційеа атака, система рівнянь зі спотвореними правими частинами над скінченним полем, інформаційна складність.*